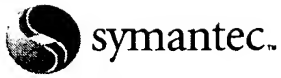
APPENDIX A



Norton™ Personal Firewall 2003

User's Guide

Norton™ Personal Firewall User's Guide

Documentation version 6.0

PN: 10025076

Copyright Notice

Standard Template Library

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

1. LICENSE:

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, you may make that number of copies of the Software licensed to you by Symantec as provided in your License Module. Your License Module shall constitute proof of your right to make such copies.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;

C. use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network; and

D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or

F. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the Software (including any subscription included with your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. SIXTY DAY MONEY BACK GUARANTEE:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty (60) day period following the delivery to you of the Software.

4. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL

PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

5. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

6. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

Contents

Chapter 4 Norton Personal Firewall basics

Chapter 5 Keeping current with LiveUpdate

Chapter 6 Controlling access to protected computers

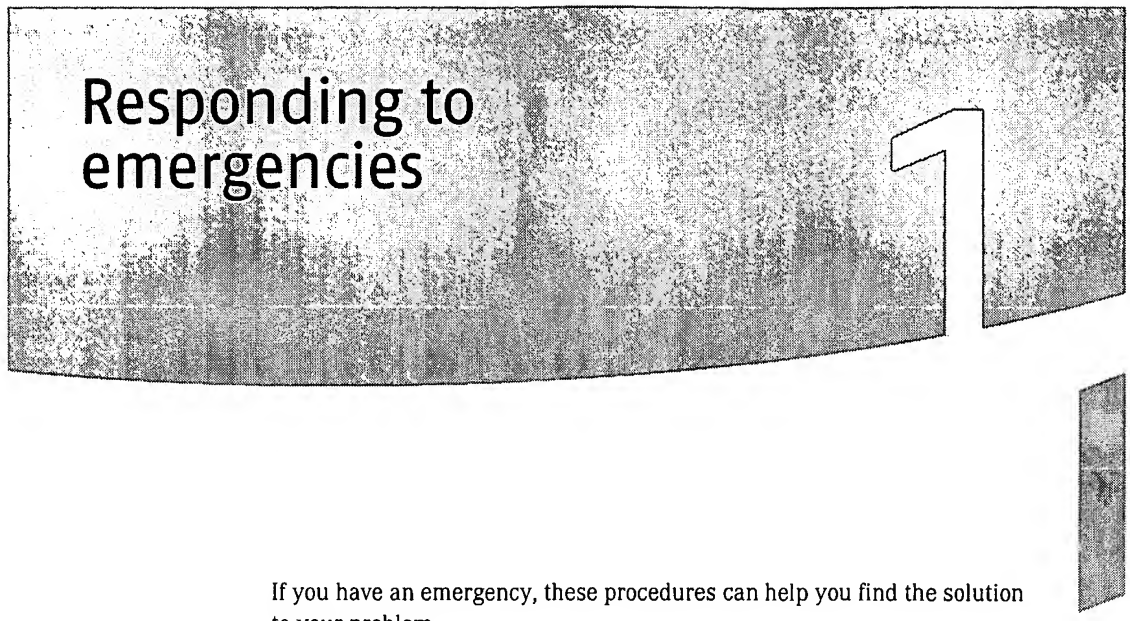
Chapter 7 Guarding against intrusion attempts

Appendix A Troubleshooting Norton Personal Firewall

Appendix B About the Internet

Appendix C Understanding Internet risks

Responding to emergencies



If you have an emergency, these procedures can help you find the solution to your problem.

If you think your computer is under attack

If your computer is behaving unpredictably, and you have determined that the behavior is not due to a virus or a corrupted file, you may be the victim of an Internet attack.

If you suspect that someone is attacking your computer, immediately disconnect your computer from the Internet. If you have not yet installed Norton Personal Firewall, install it now.

If you have installed Norton Personal Firewall, you can use its security tools to block the attack, investigate the attacker, and prevent this type of attack in the future.

To block and investigate an attack

1. Open Norton Personal Firewall.
2. Click **Block Traffic**.
   This immediately stops all incoming and outgoing communication with other computers.

See "Stop Internet communication with Block Traffic" on page 44.

3. If you are using the Security Monitor, click **Security Center**.
4. In the Security Center, click **Statistics**.
5. Click **Attacker Details**.
   Your browser opens the Visual Tracking Web page.

See "Identify the source of communications" on page 43.

6 Use Visual Tracking to identify the IP address of the computer that the attacker used.
You can use this information to report the attack to the ISP that owns the IP address.

See "Restrict a blocked computer" on page 88.

7 To block all future connections from this IP address, add this computer to your Restricted Zone.

If you suspect that the attacker has already compromised your computer, install Norton Personal Firewall, then visit http://security.symantec.com for tools to repair damage and eradicate any threats that the attacker may have placed on your computer.

Recover from an emergency

Once you've dealt with the problem, you can install Norton Personal Firewall and perform the following activities.

Action	Description
Install Norton Personal Firewall.	Norton Personal Firewall can keep your computer safe from future attacks. See "Installing Norton Personal Firewall" on page 19.
Update your protection.	After installing, run LiveUpdate to ensure that you have the most updated protection. See "Keeping current with LiveUpdate" on page 53.
Configure your firewall.	The default installation of Norton Personal Firewall should provide sufficient protection for most users, but you can customize protection by adjusting firewall settings. See "Customize firewall protection" on page 72.
Periodically review program logs and statistics.	Norton Personal Firewall maintains extensive logs of all of the actions that it takes to protect your computer. Check these logs occasionally to identify potential problems. See "Monitoring Norton Personal Firewall" on page 103.

Prevent future problems

Norton Personal Firewall can protect your computer against most Internet attacks.

To prepare your computer for emergencies:

- Stay informed about security risks by visiting the Symantec Security Response *Web site* (securityresponse.symantec.com).
- Keep your *browser* up-to-date. Software publishers release new versions to fix vulnerabilities in their browsers.
- Use *passwords* intelligently. For important information, use complex passwords that include uppercase and lowercase letters, numbers, and symbols. Don't use the same password in multiple places.
- Don't run software if you don't trust the publisher and the source from which you received the software.
- Don't open *email* attachments unless you are expecting an attachment and you trust the sender.
- Be sensible about providing personal information. Many sites ask for more information than they need.
- Review the privacy policies of the sites to which you are considering sending information.
- Tell children never to reveal details about themselves to people they meet via instant messenger programs.
- Back up files regularly and keep copies of the last few backups on hand.

About Norton Personal Firewall 2

Norton Personal Firewall protects computers from Internet attacks, guards your privacy, and speeds Web surfing by eliminating ads.

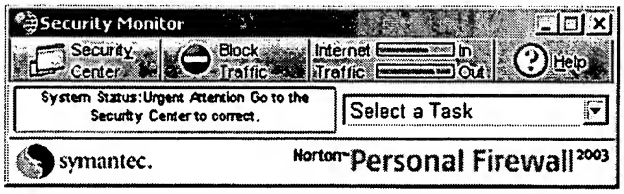
What's new in Norton Personal Firewall 2003

Norton Personal Firewall 2003 now includes:

- Security Monitor
  Gives you fast access to the most-used Norton Personal Firewall tools
- Visual Tracking
  Identifies the source of attacks and other Internet communication
- Password protection
  Provides increased security for Norton Personal Firewall options
- Block Traffic
  Lets you immediately stop other computers' ability to communicate with your computer
- Alert Assistant
  Helps you understand alerts and potential security issues
- Log Viewer
  Improved version helps you see all of the actions Norton Personal Firewall takes to protect your computer
- Privacy Control
  Enhanced version blocks private information in email and instant messages

Norton Personal Firewall features

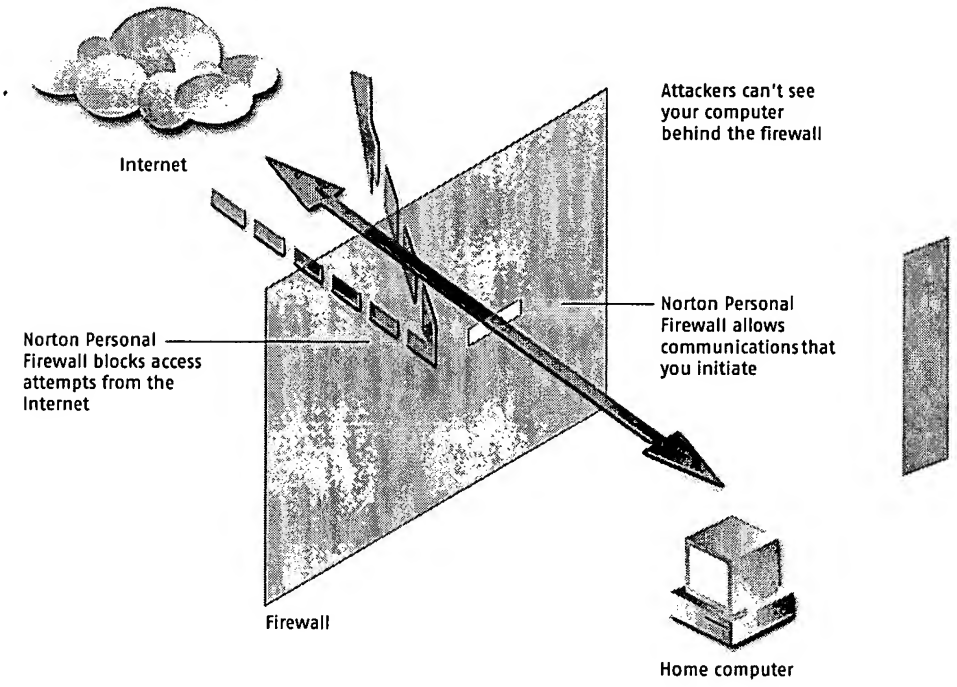
Norton Personal Firewall includes a number of security tools that help keep your computer safe. You can get fast access to all Norton Personal Firewall tools from the new Security Monitor.



Internet security can be a complicated topic to understand, so Norton Personal Firewall now includes the Alert Assistant, which helps you understand security issues, suggests how you can resolve problems, and advises you on avoiding future security problems.

About Norton Personal Firewall

Norton Personal Firewall provides a barrier between your computer and the Internet. A *firewall* prevents unauthorized users from accessing private computers and networks connected to the Internet.



Norton Personal Firewall includes features that prevent unauthorized access to your computer when you are on the Internet, detect possible Internet attacks, protect your personal information, and block Internet advertisements to speed your Internet browsing.

Norton Personal Firewall features include:

Intrusion Detection	Intrusion Detection helps keep your computer safe from Internet attacks by scanning each piece of information that enters and exits your computer. If it identifies a potential attack, Intrusion Detection alerts you and automatically blocks the connection that contained the attack. See "Guarding against intrusion attempts" on page 69.
Privacy Control	Privacy Control gives you several levels of control over the kind of information that users can send via the Web, email, and instant messenger programs. You can also control how Privacy Control reacts when Web sites attempt to set and use cookies or learn about your browser. See "Protecting your privacy" on page 89.
Ad Blocking	Ad Blocking speeds up your Web surfing by eliminating banner ads and other slow-loading or intrusive content. Norton Personal Firewall now also blocks ads made with Macromedia Flash and prevents sites from opening pop-up or pop-under ad windows. See "Blocking Internet advertisements" on page 95.

Installing Norton Personal Firewall

3

Before installing Norton Personal Firewall, take a moment to review the system requirements listed in this chapter.

System requirements

To use Norton Personal Firewall, your computer must have one of the following Windows operating systems installed:

- Windows 98, 98SE
- Windows Me
- Windows 2000 Professional
- Windows XP Professional or Windows XP Home Edition

Windows 95 and NT, the server editions of Windows 2000/XP, and the Windows XP 64-bit edition are not supported.

Your computer must also meet the following minimum requirements.

Operating System	Requirements
Windows 98/ 98SE/Me	■ Intel Pentium processor (or compatible) at 150 MHz or higher ■ 48 MB of RAM (64 MB recommended) ■ 25 MB of available hard disk space ■ Internet Explorer 5.01 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive
Windows 2000 Professional	■ Intel Pentium processor (or compatible) at 150 MHz or higher ■ 48 MB of RAM (64 MB recommended) ■ 25 MB of available hard disk space ■ Internet Explorer 5.01 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive
Windows XP Professional or Home Edition	■ Intel Pentium II processor (or compatible) at 300 MHz or higher ■ 48 MB of RAM (64 MB recommended) ■ 25 MB of available hard disk space ■ Internet Explorer 5.01 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive

Supported email clients

Norton Personal Firewall can scan email messages for private information in any POP3-compatible email client, including:

- Microsoft® Outlook® Express 4.0/5.X
- Microsoft Outlook 97/98/2000/XP
- Netscape® Messenger 4.X, Netscape Mail 6.0
- Eudora® Light 3.0, Eudora Pro 4.0, Eudora 5.0

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients
- POP3s that use SSL (Secure Sockets Layer)
- Web-based email such as Hotmail and Yahoo!
- Lotus Notes mail

Supported instant messenger clients

Norton Personal Firewall can scan for private information in the following instant messengers:

- AOL Instant Messenger, version 4.3 or later
- MSN Instant Messenger, version 3.6 or later
- Windows Messenger, version 4.0 or later

Before installation

Before you install Norton Personal Firewall, prepare your computer.

Prepare your computer

See "If you need to uninstall Norton Personal Firewall" on page 34.

If you have an older version of Norton Personal Firewall, the new version prompts you to remove the older version. If you have a recent version of Norton Personal Firewall, you can transfer your existing settings to the new version of the program.

Quit all other Windows programs before installing Norton Personal Firewall. Other active programs may interfere with the installation and reduce your protection.

If you're using Windows XP

Windows XP includes a *firewall* that can interfere with Norton Personal Firewall protection features. You must disable the Windows XP firewall before installing Norton Personal Firewall.

To disable the Windows XP firewall

1. On the Windows XP taskbar, click **Start > Control Panel > Network Connections**.
2. If you have created more than one modem or network connection, select the active connection.
3. Click **Network Tasks**.
4. Click **Change settings of this connection**.
5. On the Advanced tab, in the Internet Connection Firewall section, uncheck **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
6. Click **OK** to close the settings window.
7. Click **OK** to close the Network Tasks window.

Install Norton Personal Firewall

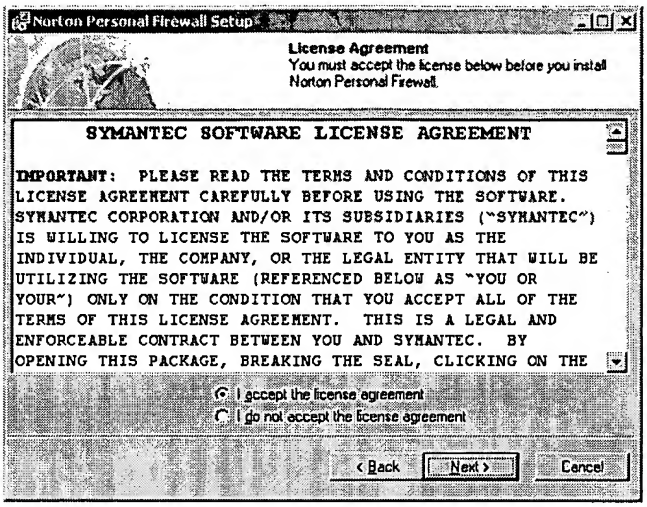
Install Norton Personal Firewall from the Norton Personal Firewall CD. Install a copy of Norton Personal Firewall on each computer that you want to protect.

To install Norton Personal Firewall

1. Insert the Norton Personal Firewall CD into the CD-ROM drive.
2. In the Norton Personal Firewall CD window, click **Install Norton Personal Firewall**.
   If your computer is not set to automatically run a CD, you must manually open it.
   The first installation window reminds you to close all other Windows programs.

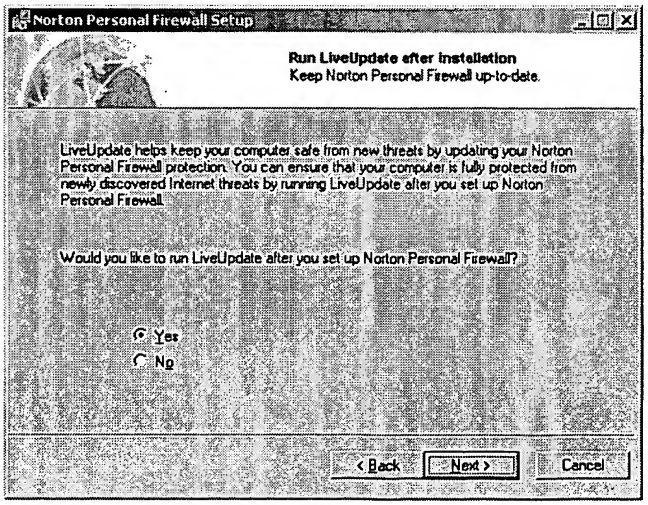
See "If the opening screen does not appear" on page 25.

3 Click **Next**.



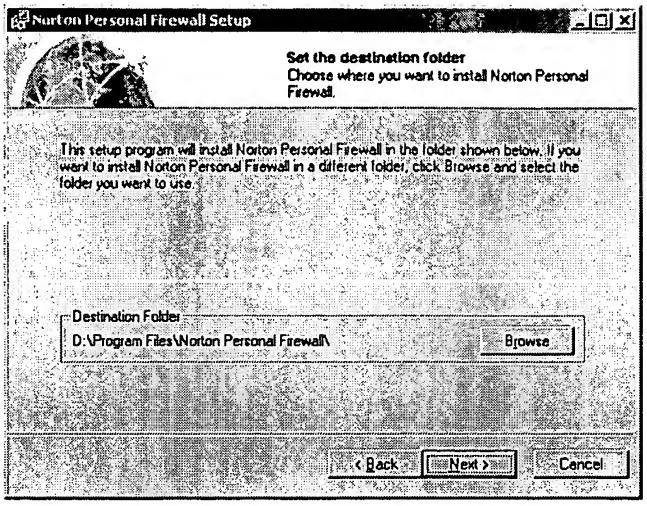
4 Read the License Agreement, then click **I accept the license agreement**.
If you decline, you cannot continue with the installation.

5 Click **Next**.



6 In the Run LiveUpdate after installation window, select whether you want to run LiveUpdate after the installation is done.

7 Click **Next**.

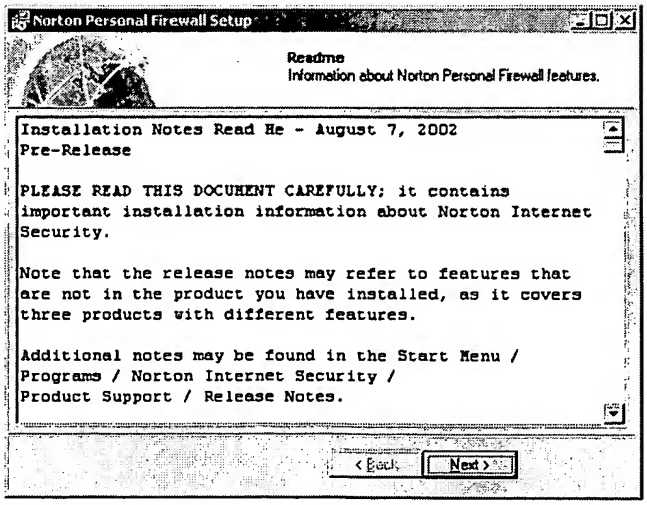


8 Click **Browse** to select a folder into which you want to install Norton Personal Firewall, if it is other than the default location.

9 Click **Next**.

See "Register your software" on page 25.

10 Click **Next** to begin installing Norton Personal Firewall.
After Norton Personal Firewall is installed, the Registration Wizard appears.



11 Read the readme text, then click **Next**.

12 Click **Finish** to complete the installation.

If the opening screen does not appear

Sometimes a computer's CD-ROM drive does not automatically run a CD.

To start the installation from the Norton Personal Firewall CD

1 On your desktop, double-click **My Computer**.

2 In the My Computer window, double-click the icon for your CD-ROM drive.

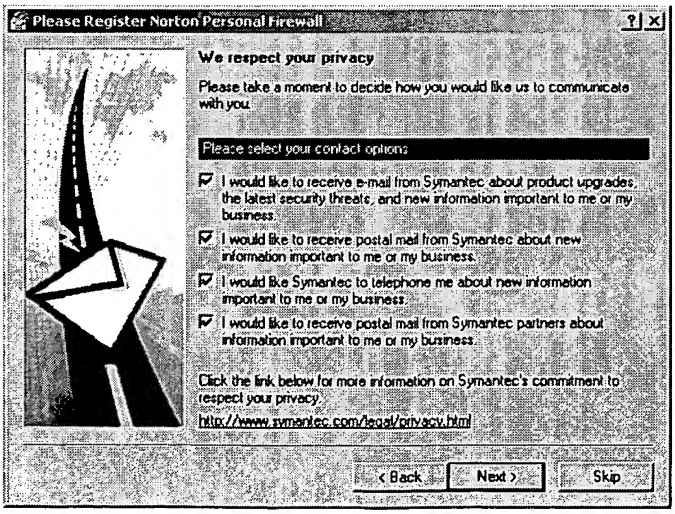
3 In the list of files, double-click **Cdstart.exe**.

Register your software

Use the Registration Wizard to register your software online. If you skip online registration, you can register your software later using the Product Registration option on the Help menu.

To register your software

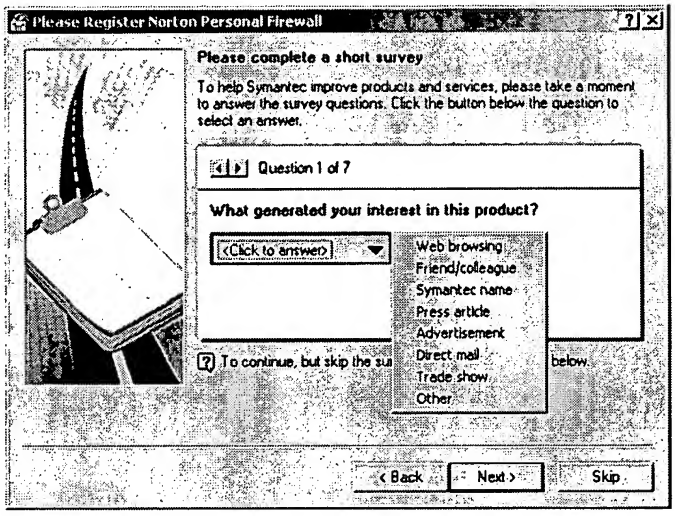
1 In the first Registration window, select the country from which you are registering and the country in which you live (if different), then click **Next**.



2 If you would like information from Symantec about Norton Personal Firewall, select the method by which you want to receive that information, then click **Next**.

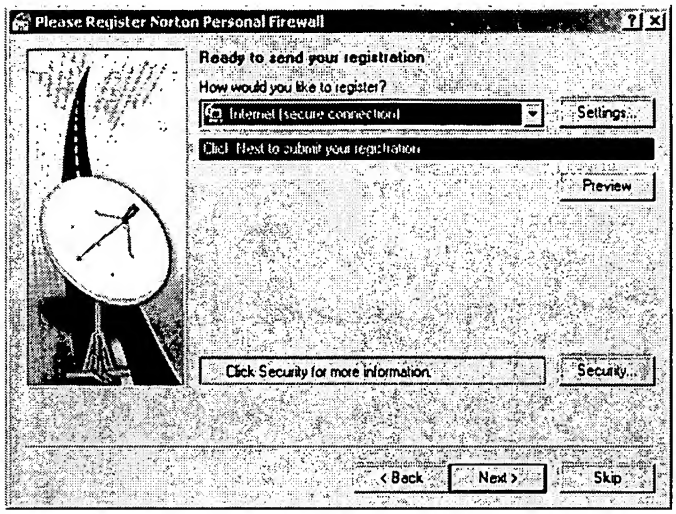
3 Type your name, then click **Next**.

4 Type your address, then click **Next**.



5 Do one of the following:

- Answer the survey questions to help Symantec improve its products and services, then click **Next**.
- Skip the survey by clicking **Next**.



6 Select whether you want to register Norton Personal Firewall over the Internet or by mail.
If you want to register by mail, your computer must be connected to a printer that the Registration Wizard can use to print the registration form. If you want to register using the Internet, you must be connected to the Internet.

7 Click **Next**.

8 To get a copy of your registration information for future reference, do one of the following:

- Write down the serial number.
- Click **Print**.

9 Click **Next**.

10 Select whether you want to use your existing profile the next time that you register a Symantec product, or type the information as part of registration.

11 Click **Finish**.

After installation

After Norton Personal Firewall is installed, a prompt appears giving you the option to restart your computer immediately. After restarting, the Security Assistant appears to guide you through the configuration of Norton Personal Firewall.

Restart your computer

After installation, a prompt appears telling you that you must restart your computer for the updates to take effect.

To restart your computer

- In the Installer Information dialog box, click **Yes**.
  Configuration of Norton Personal Firewall is not complete until you restart your computer.

Use the Security Assistant

The Security Assistant helps you quickly configure your Norton Personal Firewall protection. The Security Assistant is divided into four categories:

- Home Networking
- Program Control
- Privacy Control
- Password Protection

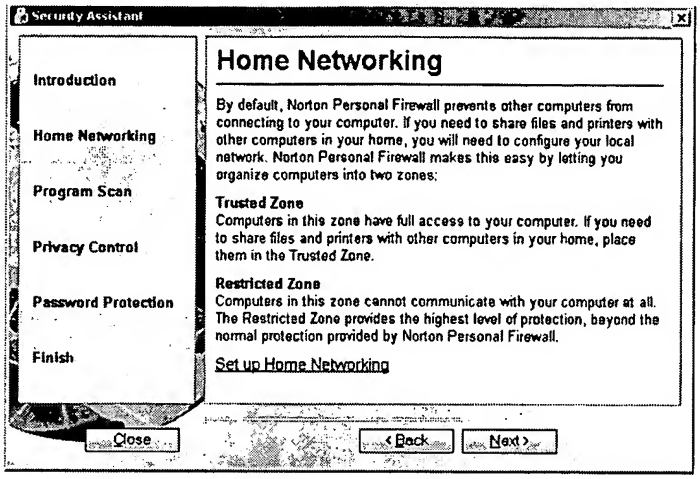
Set up Home Networking

See "Connect to a network" on page 61.

Use Home Networking to identify computers to which you want to grant access to your computer and those to which you want to deny access. The Home Network Wizard can automatically configure your *network* and add computers to your Trusted Zone.

To set up Home Networking

1 In the Security Assistant Roadmap, click **Home Networking**.



2 In the Home Networking pane, click **Set up Home Networking**.

3 In the Home Networking Wizard, click **Next**.

4 Follow the on-screen instructions to configure your network.

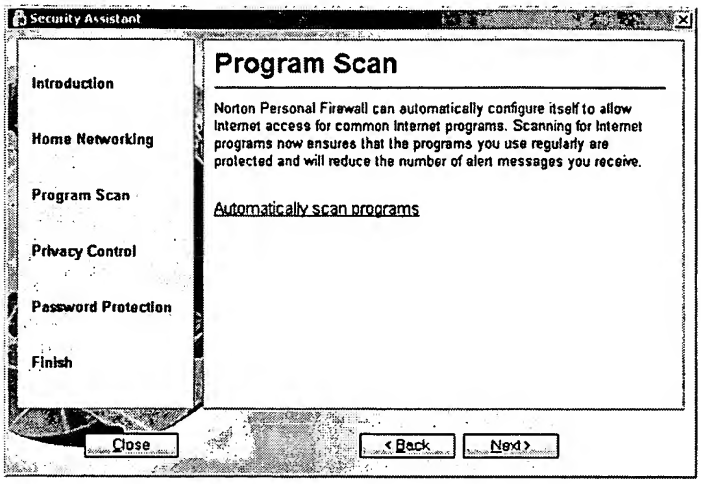
Set up Program Control

See "Scan for Internet-enabled programs" on page 77.

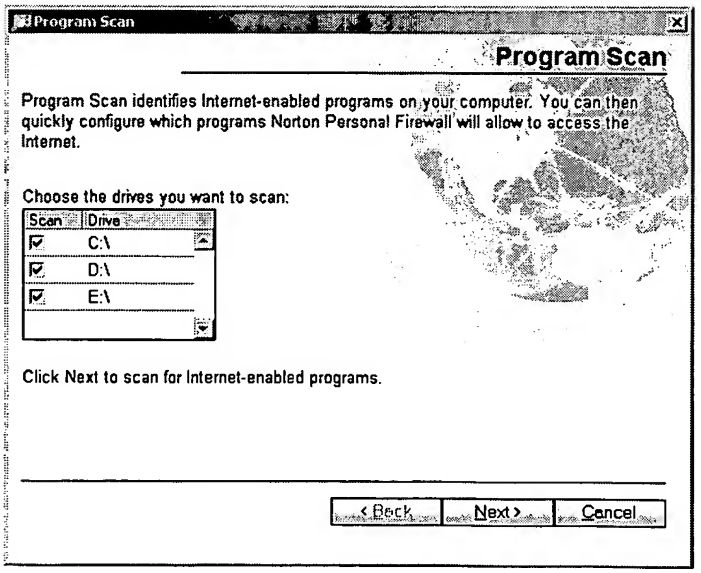
Norton Personal Firewall can scan your computer for Internet-enabled programs and create access rules for them. When the scan is complete, you can use the results to determine which programs should have access to the Internet and, if desired, adjust their access rules.

To set up Program Control

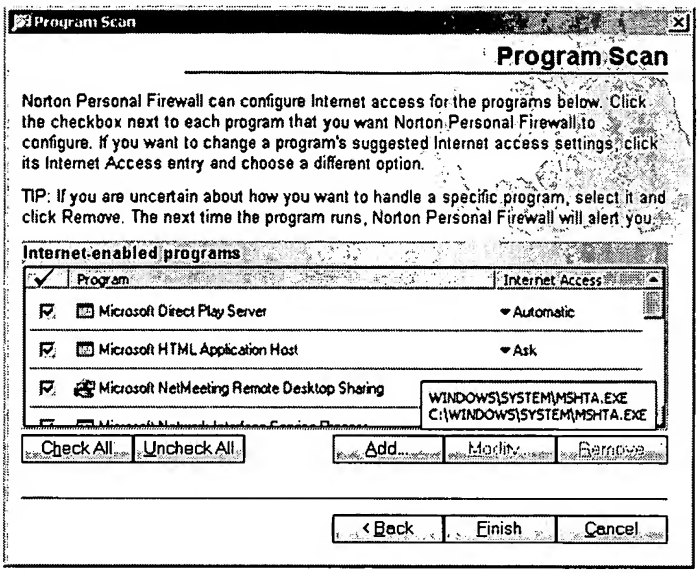
1 In the Security Assistant Roadmap, click **Program Scan**.



2 In the Program Scan pane, click **Automatically scan programs**.



3 In the Program Scan window, click **Next** to begin the scan.
When the scan is complete, all Internet-enabled programs that were found are listed.



4 To allow Internet access for a program, check the check box to the left of the program's name.

5 To change the Internet access rule or category of a program, in the Internet Access or Category drop-down lists, select the setting that you want.

6 Click **Finish** when you are done.

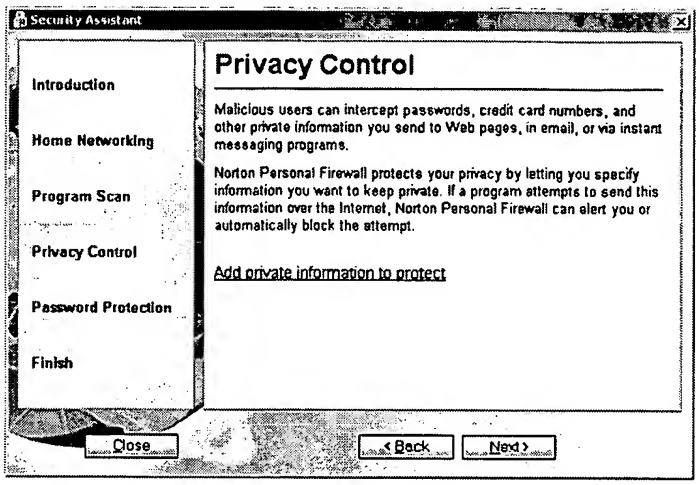
Set up Privacy Control

See "Identify private information to protect" on page 89.

Using Privacy Control, you can identify private information that should have extra protection. Privacy Control can then prevent users from sending this information to *Web sites*, in *email* messages and attached Microsoft Office files, and through supported instant messenger programs.

To set up Privacy Control

1 In the Security Assistant Roadmap, click **Privacy Control**.



2 In the Privacy Control pane, click **Add private information to protect**.

3 In the Add Private Information dialog box, under Type of information to protect, select a category.

4 In the Descriptive name text box, type a description to help you remember why you are protecting the data.

5 In the Information to protect text box, type the last five or six characters of the information that you want to block from being sent over nonsecure Internet connections.
By entering only partial information, you ensure that untrustworthy people with physical access to your computer cannot steal entire credit card numbers and other information.

6 Click **OK**.

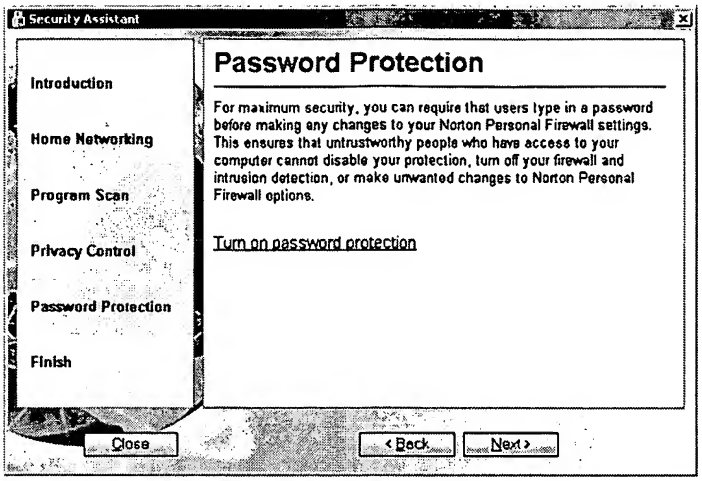
Set up Password Protection

See "Use the Security Monitor" on page 38.

For maximum security, you can require a *password* before allowing anyone to make a change to your Norton Personal Firewall settings. This ensures that only the people you trust are able to disable your protection, turn off your *firewall* and intrusion detection, or make changes to Norton Personal Firewall options.

To protect Norton Personal Firewall options with a password

1 In the Security Assistant Roadmap, click **Password Protection**.



2 In the Password Protection pane, click **Turn on password protection**.

3 In the Password and Confirm Password text boxes, type a password.

4 Click **OK**.

If you have Norton SystemWorks installed

If you have Norton SystemWorks installed on your computer when you install Norton Personal Firewall, the installer adds a Norton Personal Firewall tab to the Norton SystemWorks main window and a Norton SystemWorks tab to the Security Center.

To open Norton Personal Firewall from Norton SystemWorks

1 Open Norton SystemWorks.

2 On the Norton Personal Firewall tab, click **Launch Norton Personal Firewall**.

To open Norton SystemWorks from Norton Personal Firewall

1 Open Norton Personal Firewall.

2 In the Security Center, on the Norton SystemWorks tab, click **Launch Norton SystemWorks**.

If you need to uninstall Norton Personal Firewall

If you need to uninstall Norton Personal Firewall from your computer, use the Uninstall Norton Personal Firewall option on the Windows Start menu.

During uninstall, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

To uninstall Norton Personal Firewall

1. Do one of the following:
   - On the Windows taskbar, click **Start > Programs > Norton Personal Firewall > Uninstall Norton Personal Firewall**.
   - On the Windows XP taskbar, click **Start > More Programs > Norton Personal Firewall > Uninstall Norton Personal Firewall**.
2. Click **Next**.
3. In the Installer Information dialog box, click **Yes** to restart your computer.

If you have no other Symantec products on your computer, you should also uninstall LiveReg and LiveUpdate.

To uninstall LiveReg and LiveUpdate

1. Do one of the following:
   - On the Windows taskbar, click **Start > Settings > Control Panel**.
   - On the Windows XP taskbar, click **Start > Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.
3. In the list of currently installed programs, click **LiveReg**.
4. Do one of the following:
   - In Windows 2000/Me, click **Change/Remove**.
   - In Windows 98, click **Add/Remove**.
   - In Windows XP, click **Remove**.
5. Click **Yes** to confirm that you want to uninstall the product.
6. To uninstall LiveUpdate, repeat steps 1 through 5, selecting LiveUpdate in step 3.

Norton Personal Firewall basics

4

After installation, Norton Personal Firewall automatically protects any computer on which it is installed. You do not have to start the program to be protected.

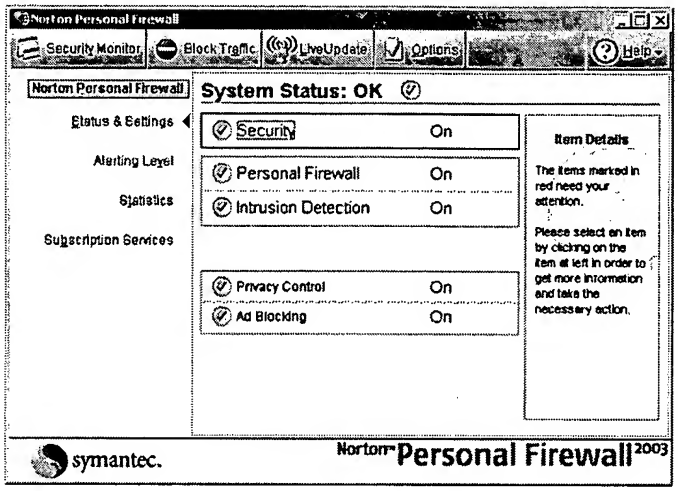
Access Norton Personal Firewall

Launch Norton Personal Firewall to change protection settings or monitor its activities.

To access Norton Personal Firewall

- Do one of the following:
  - On the Windows taskbar, click **Start > Programs > Norton Personal Firewall > Norton Personal Firewall**.

- On the Windows XP taskbar, click **Start > More Programs > Norton Personal Firewall > Norton Personal Firewall.**
- On the Windows desktop, double-click **Norton Personal Firewall.**



Access Norton Personal Firewall from the system tray

Norton Personal Firewall adds an icon to the Windows system tray. On most computers, the system tray is at the far right of the Windows taskbar at the bottom of your screen. Click this icon to open a menu containing frequently used Norton Personal Firewall tools.

To use the Norton Personal Firewall system tray menu

1. In the system tray, right-click the Norton Personal Firewall icon.
2. In the menu that appears, select an item. Items in the menu include:

Norton Personal Firewall	Opens a Norton Personal Firewall window.
Hide/View Alert Tracker	Displays or hides the Alert Tracker. See "Use Alert Tracker" on page 41.
Block Traffic	Immediately stops all incoming and outgoing information. See "Stop Internet communication with Block Traffic" on page 44.

About Norton Personal Firewall	Displays detailed information about Norton Personal Firewall components.
LiveUpdate	Updates your protection. See "Keeping current with LiveUpdate" on page 53.
Help	Displays the Norton Personal Firewall online Help. See "Use online Help" on page 48.
Disable	Turns off all Norton Personal Firewall protection features. See "Temporarily disable Norton Personal Firewall" on page 47.

See "About Global Settings" on page 46.

Use the Norton Personal Firewall Options to add additional tools to the menu.

Work with Norton Personal Firewall

Norton Personal Firewall works in the background, so you may only interact with the program when it alerts you of new network *connections* and possible problems. You can choose to view the new Security Monitor or the standard Security Center window, respond to security problems, and control the number of *alerts* you receive and how the program resolves potential security problems.

Access Norton Personal Firewall protection features

The default settings for Norton Personal Firewall provide a safe, automatic, and efficient way of protecting your computer. If you want to change or customize your protection, you can access all Norton Personal Firewall tools from the Status & Settings window.

To change settings for individual features

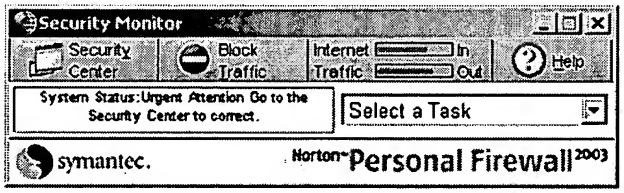
1. Open Norton Personal Firewall.
2. If you have chosen to view the Security Monitor, click **Security Center**.

3 In the Security Center, do one of the following:
   - Double-click a feature you want to customize.
   - Select a feature, then in the lower-right corner of the window, click **Customize**.
4 Configure the feature.
5 When you are done making changes, click **OK**.

Use the Security Monitor

The Security Monitor collects the most-used Norton Personal Firewall tools into a compact window. When you're online, place the Security Monitor window in an unused part of your screen. This lets you monitor your *connection*, view information about security events, and personalize your protection without requiring a lot of space on your screen.

When you start Norton Personal Firewall, it launches the Security Center. You can then switch to the Security Monitor.



To view the Security Monitor

- In the Security Center, in the upper-left corner, click **Security Monitor**.

To view the Security Center

- In the Security Monitor, in the upper-left corner, click **Security Center**.

Select a task with the Security Monitor

Use the Select a Task menu in the Security Monitor to quickly perform common Norton Personal Firewall tasks. The Select a Task menu includes:

Task	More information
Test security	See "Check your computer's vulnerability to attack" on page 42.
Edit private information	See "Protecting your privacy" on page 89.
View Log Viewer	See "View Norton Personal Firewall Logs" on page 107.
Run LiveUpdate	See "Keeping current with LiveUpdate" on page 53.
Run Program Scan	See "Scan for Internet-enabled programs" on page 77.
Setup Home Network	See "Organize computers into network zones" on page 62.

Respond to Norton Personal Firewall alerts

Norton Personal Firewall monitors communication activities to and from your computer and lets you know when an activity that may compromise your security is taking place.

When an *alert* appears, read it before you make a decision. Identify what type of alert it is and the threat level. Once you understand the risks, you can make a choice.

Take as much time as you need to make your choice. Your computer is safe from attack while the alert is active.

Norton Personal Firewall helps you decide on an appropriate action by preselecting the recommended action if one exists. Norton Personal Firewall cannot suggest recommended actions for all alerts.

Learn more with the Alert Assistant

Each Norton Personal Firewall alert includes a link to the Alert Assistant. The Alert Assistant includes customized information about each alert, including:

- The type of alert
- The threat level
- The communication that triggered this alert

- What these types of alerts indicate
- How to reduce the number of these alerts you receive

To use the Alert Assistant

1. In any alert window, click the Alert Assistant button.
2. In the Alert Assistant window, review the information about this alert.
3. To respond to the alert, close the Alert Assistant.

Adjust the Alerting Level

The Alerting Level slider lets you control the amount of information that Norton Personal Firewall *logs* and the number of alerts that it displays.

Your options are:

Alerting Level	Information provided	Alert Tracker messages	Security Alerts	Notifies you when...
Minimal	Critical Internet events	None	Logged, not displayed	Program Control rules are created automatically. Port scans occur. Confidential information is blocked. A remote access Trojan horse program is encountered.
Medium	Important Internet events	Some	Logged, not displayed	Same notification as Minimal, plus: ▪ Programs access the Internet.
High	Important Internet events and complete program activities	Many	Logged and displayed	Same notification as Medium, plus: ▪ Unused ports are blocked. ▪ Cookies and content are blocked.

To adjust the Alerting Level

1. Open Norton Personal Firewall.
2. In the Security Center, click **Alerting Level**.
3. Move the slider to choose an Alerting Level.

Use Alert Tracker

Many of the Internet events that Norton Personal Firewall monitors are not significant enough to trigger alerts. Alert Tracker provides an easy way to monitor these less-important security events.

Alert Tracker displays the same information that appears in the Security Event field on the Security Monitor. This allows you to monitor your computer's security without having to keep the Security Monitor visible at all times. Alert Tracker also provides a quick way to remove ads from *Web pages*.

If you choose to display Alert Tracker, it attaches to either side of the screen on your primary monitor. When a security event occurs, Alert Tracker displays a message for a few seconds and then returns to the side of the screen. If you miss an Alert Tracker message, you can review a list of recent messages.

See "Use the Ad Trashcan" on page 98.

Alert Tracker also contains the Ad Trashcan, which is part of the Norton Personal Firewall Ad Blocking feature.

To view or hide Alert Tracker

1. Open Norton Personal Firewall.
2. In the Security Center, click **Options** > **Internet Security**.
3. On the General tab, do one of the following:
   - Check **Show the Alert Tracker** to view Alert Tracker.
   - Uncheck **Show the Alert Tracker** to hide Alert Tracker.
4. Click **OK**.

To review recent Alert Tracker messages

1. On the Windows desktop, double-click the Alert Tracker.
2. To the right of the first message, click the arrow if it appears.
3. Double-click an entry to open the Log Viewer.

See "Review detailed statistics" on page 105.

To move Alert Tracker

- Drag the half globe to the side of the screen on which you want it to appear.

To hide Alert Tracker from the system tray menu

- In the Windows system tray, right-click the Norton Personal Firewall icon, then click **Hide Alert Tracker**.

If you hide Alert Tracker, you will not be notified when your computer joins a *network*. Information about the *connection* will still appear in the *logs*.

Check your computer's vulnerability to attack

Use Security Check to test your computer's vulnerability to security intrusions. The Security Check link in Norton Personal Firewall connects you to the Symantec *Web site*, where you can scan for vulnerabilities and get detailed information about Security Check scans.

You must be connected to the Internet to check your computer's vulnerability.

To check your computer's vulnerability to attack

1. Open Norton Personal Firewall.
2. Do one of the following:
   - In the Security Center, click **Security**, then click **Check Security**.
   - In the Security Monitor window, on the Select a Task menu, click **Test Security**.
3. On the Security Check Web page, click **Scan for Security Risks**.
4. To learn more about the Security Check tests, click **About Scan for Security Risks**.

When the scan is complete, the results page lists all of the areas that were checked and your level of vulnerability in each one. For any area marked as at risk, you can get more details about the problem and how to fix it.

To get more information about an at-risk area

- ❖ On the results page, next to the scan name, click **Show Details**.

Identify the source of communications

Visual Tracking helps you learn more about computers that attempt to connect to your computer. Using Visual Tracking, you can identify the location of the *IP address* used and contact information for the owner of the address. You can use this information to identify the origin of an attack and to learn more about intrusion attempts.

You can trace *connection attempts* from three places in Norton Personal Firewall:

- Statistics
- Log Viewer
- AutoBlock

To trace a connection attempt from Statistics

1. Open Norton Personal Firewall.
2. In the Security Center, click **Statistics**.
3. Click **Attacker Details**.
   Your browser opens the Visual Tracking Web page.

To trace a connection attempt from the Log Viewer

1. Open Norton Personal Firewall.
2. In the Security Center, click **Statistics**.
3. Click **View Logs**.
4. In the left column of the Log Viewer window, under Internet Security, click **Connections**.
5. In the right column of the Log Viewer window, select a connection you want to trace.
6. At the bottom of the Log Viewer window, click the computer's IP address or name.
   Your browser opens the Visual Tracking Web page.

To trace a connection attempt from AutoBlock

1. Open Norton Personal Firewall.
2. In the Security Center, double-click **Intrusion Detection**.

3 In the Intrusion Detection window, in the AutoBlock section, select a connection you want to trace.

4 Click **Attacker Details**.
Your browser opens the Visual Tracking Web page.

When Visual Tracking is finished, it displays a visual representation of where this communication originated and contact information for the owner of the IP address.

Stop Internet communication with Block Traffic

The Security Center and the Security Monitor include a Block Traffic button that lets you immediately halt any communication between your computer and another. This can be a handy way to limit any damage to your computer if it is attacked, if a *Trojan horse* is sending personal information without your permission, or if you inadvertently allow an untrusted person to access files on your computer.

When this option is active, Norton Personal Firewall stops all communication to and from your computer. To the outside world, it appears that your computer has completely disconnected from the Internet.

If you want to block all traffic into and out of your computer, Block Traffic is more effective than simply using your Internet software to disconnect. Most Internet programs can automatically connect without any input from the user, so a malicious program could reconnect when you are away from the computer.

Block Traffic is meant to be used as a temporary measure while you address a security problem. If you restart your computer, Norton Personal Firewall automatically allows all incoming and outgoing communication. To continue blocking traffic, click the Block Traffic button in the Security Center or Security Monitor.

To avoid attack while fixing security problems

1 Open Norton Personal Firewall.

2 In the Security Center or the Security Monitor window, click **Block Traffic**.

3 Use Norton Personal Firewall tools to address the security problem.

4 When you have fixed the problem, click **Allow Traffic**.

Customize Norton Personal Firewall

The default Norton Personal Firewall settings should provide adequate protection for most users. If you need to make changes, use the Options menu to access Norton Personal Firewall options. The options let you control more advanced settings.

If you are using Windows 2000/XP and you do not have Local Administrator access, you cannot change Norton Personal Firewall options.

To customize Norton Personal Firewall

1. Open Norton Personal Firewall.
2. At the top of the Security Center, click **Options**.
3. Select the tab on which you want to change options.

About General options

General options let you control when Norton Personal Firewall runs, protect program settings with a *password*, and choose visual elements you want to display.

About LiveUpdate options

See "Keeping current with LiveUpdate" on page 53.

LiveUpdate options let you enable and disable Automatic LiveUpdate, which automatically checks for Norton Personal Firewall updates when you are connected to the Internet. For maximum security, you should leave this option checked.

You can choose the Norton Personal Firewall components you want Automatic LiveUpdate to monitor. You can also choose whether Automatic LiveUpdate updates the components in the background or alerts you that there are updates available.

About Firewall options

Firewall options let you activate advanced protection features and customize the ports your computer uses to view *Web pages*. Most people will not need to make any changes to these settings.

About Web Content options

Web Content options let you control how Norton Personal Firewall handles interactive online content, ads, and possible privacy intrusions. Web Content options are arranged on three tabs.

About Global Settings

Global Settings let you control the default actions Norton Personal Firewall takes when Web sites attempt to get information about your *browser* or use animated images, JavaScripts, and other *active content.*

About User Settings

User Settings let you customize *cookie* blocking, pop-up window blocking, and *ActiveX* and *Java* settings for individual sites.

About Ad Blocking settings

Ad Blocking settings let you specify individual *ad banners* or groups of ad images you want to block or allow on individual sites. See "Use text strings to identify ads to block or permit" on page 99.

About Email options

Email options let you control how Norton Personal Firewall notifies you when it is scanning email messages for private information.

Password-protect options

You can protect Norton Personal Firewall options with a *password.* This ensures that only the people you trust are able to make changes to your options.

To protect Norton Personal Firewall options with a password

1. Open Norton Personal Firewall.
2. At the top of the Norton Personal Firewall window, click **Options** > **Internet Security**.
3. On the General tab, check **Turn on Password Protection**.
4. In the Password and Confirm Password text boxes, type a password.
5. Click **OK**.

Reset options password

If you forget your options password you can reset it.

To reset your Norton Personal Firewall options password

1. Do one of the following:
   - On the Windows taskbar, click **Start > Programs > Norton Personal Firewall > Uninstall Norton Personal Firewall**.
   - On the Windows XP taskbar, click **Start > More Programs > Norton Personal Firewall > Uninstall Norton Personal Firewall**.
2. In the Remove Application window, click **Reset Password**.
3. In the password reset dialog box, in the Reset Password Key text box, type the Reset Password Key that appears above the text box.
   The Reset Password Key is case-sensitive.
4. In the New Password and Confirm New Password text boxes, type a new password.
5. Click **OK**.
6. In the Remove Application window, click **Cancel**.
7. In the Norton Personal Firewall alert, click **Exit**.
8. In the Setup Canceled alert, click **OK**.

Temporarily disable Norton Personal Firewall

There may be times when you want to temporarily disable Norton Personal Firewall or one of its features. For example, you might want to view online ads or see if Norton Personal Firewall is preventing a *Web page* from appearing correctly.

Disabling Norton Personal Firewall also disables all of the individual features.

To temporarily disable Norton Personal Firewall

1. Open Norton Personal Firewall.
2. In the Security Center, click **Security**.
3. On the right side of the screen, click **Turn Off**.

Norton Personal Firewall is automatically turned back on the next time you start your computer.

You can also disable individual security features. For example, you might want to see if the Personal Firewall is preventing a program from operating correctly.

To disable a protection feature

1 Open Norton Personal Firewall.

2 In the Security Center, select the feature that you want to disable.

3 On the right side of the screen, click **Turn Off**.

For more information

Norton Personal Firewall provides glossary terms, online Help, this User's Guide in PDF format, tutorials on the *Web*, and links to the Knowledge Base on the Symantec *Web site*.

Look up glossary terms

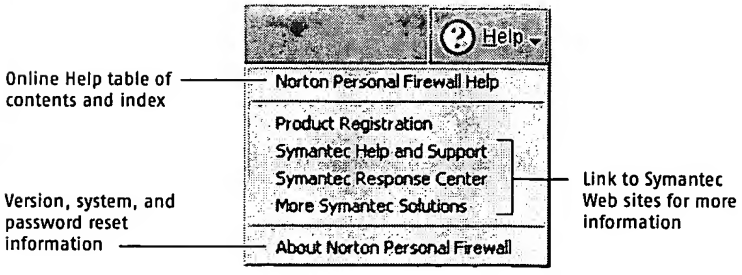
Technical terms that are italicized in the User's Guide are defined in the glossary, which is available in both the User's Guide PDF and Help. In both locations, clicking a glossary term takes you to its definition.

Use online Help

Help is always available throughout Norton Personal Firewall. Help buttons or links to more information provide information specific to the task you are completing. The Help menu provides a comprehensive guide to all product features and tasks you can complete.

To access Help

1 At the top of the Norton Personal Firewall main window, click **Help**.



2 On the main Help menu, click **Norton Personal Firewall Help**.

3 In the left pane of the Help window, select one of the following tabs:
   - Contents: Displays the Help by topic.
   - Index: Lists Help topics in alphabetical order by key word.
   - Search: Opens a search field where you can enter a word or phrase.

Window and dialog box Help

Window and dialog box Help provides information about the Norton Personal Firewall program. This type of Help is context-sensitive, meaning that it provides help for the dialog box or window that you are currently using.

To access window or dialog box Help

- Do one of the following:
   - Click the **Tell Me More** link if one is available.
   - In the dialog box, click **Help**.

Readme file and Release Notes

The Readme file contains information about installation and compatibility issues. The Release Notes contain technical tips and information about product changes that occurred after this guide went to press. They are installed on your hard disk in the same location as the Norton Personal Firewall product files.

To read the Readme file

1 Do one of the following:
   - On the Windows taskbar, click **Start > Programs > Norton Personal Firewall > Product Support > Readme.txt**.
   - On the Windows XP taskbar, click **Start > More Programs > Norton Personal Firewall > Product Support > Readme.txt**.

   The file opens in Notepad.

2 Close the word processing program when you are done reading the file.

The Release Notes can be accessed from the Start menu.

To read the Release Notes

1 Do one of the following:

- On the Windows taskbar, click **Start > Programs > Norton Personal Firewall > Product Support > Norton Personal Firewall Release Notes**.
- On the Windows XP taskbar, click **Start > More Programs > Norton Personal Firewall > Product Support > Norton Personal Firewall Release Notes**.

The file opens in Notepad.

2 Close the word processing program when you are done reading the file.

Use the User's Guide PDF

This User's Guide is provided on the Norton Personal Firewall CD in PDF format. You must have Adobe Acrobat Reader installed on your computer to read the PDF.

To install Adobe Acrobat Reader

1 Insert the Norton Personal Firewall CD into the CD-ROM drive.

2 Click **Browse CD**.

3 Double-click the **Manual** folder.

4 Double-click the **Acrobat** folder.

5 Double-click **ar500enu.exe**.

6 Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

Once you have installed Adobe Acrobat Reader, you can read the PDF from the CD.

To read the User's Guide PDF from the CD

1 Insert the Norton Personal Firewall CD into the CD-ROM drive.

2 Click **Browse CD**.

3 Double-click the **Manual** folder.

4 Double-click **NPF2003.pdf**.

You can also copy the User's Guide to your hard disk and read it from there. It needs approximately 2.25 MB of disk space.

To read the User's Guide from your hard disk

1 Open the location into which you copied the PDF.

2 Double-click **NPF2003.pdf**.

About Norton Personal Firewall on the Web

The Symantec Web site provides extensive information about Norton Personal Firewall. There are several ways to access the Symantec Web site.

To access the Symantec Web site from the Norton Personal Firewall main window

1 Click **Help**.

2 Select one of the following:

- Technical Support Web site: Takes you to the Technical Support page of the Symantec Web site, from which you can search for solutions to specific problems, update your virus protection, and read the latest information about antivirus technology.
- Visit the Symantec Web site: Takes you to the home page of the Symantec Web site, from which you can get product information on every Symantec product.

You can always access the Symantec Web site through your Internet browser.

To access the Symantec Web site in your browser

❖ Type the Symantec Web site address, www.symantec.com.

Explore online tutorials

Symantec provides online tutorials that you can use to review many common tasks that Norton Personal Firewall performs.

To explore the online tutorials

1 Point your browser to www.symantec.com/techsupp/tutorials.html

2 On the tutorials Web page, select the product and version for which you want a tutorial.

3 Click **continue**.

4 In the list of available tutorials for your product, select the one that you want to review.

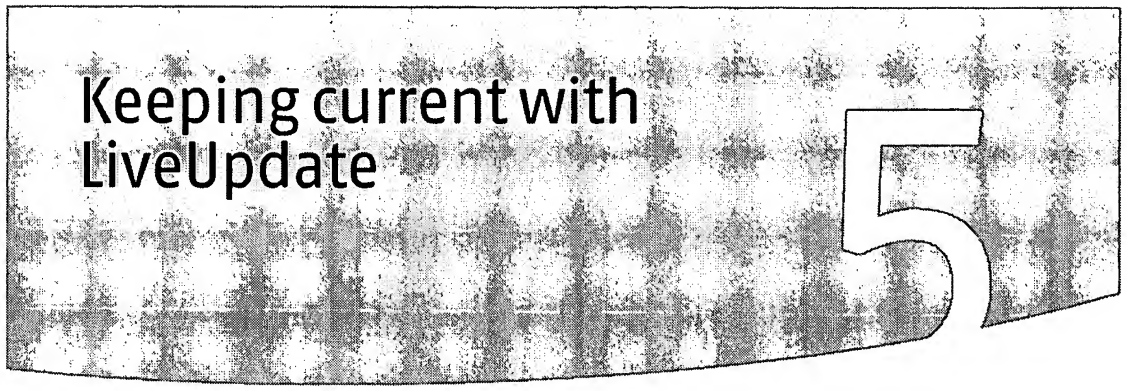
Subscribe to the Symantec Security Response newsletter

Each month, Symantec publishes a free electronic newsletter that is focused on the needs of Internet security customers. It discusses the latest antivirus technology produced by Symantec Security Response, common viruses, trends in virus workings, virus outbreak warnings, and special virus definition releases.

To subscribe to the Symantec Security Response newsletter

1. Point your browser to securityresponse.symantec.com
2. On the security response Web page, scroll down to the reference area of the page, then click **Newsletter**.
3. On the security response newsletter Web page, choose the language in which you want to receive the newsletter.
4. On the subscribe Web page, type the information requested, then click **Subscribe**.

Keeping current with LiveUpdate



Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate obtains program updates and protection updates for your computer.

Your normal Internet access fees apply when you use LiveUpdate.

If you are using Norton Personal Firewall on Windows 2000/XP, you must have Administrator access rights to run LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of obtaining and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the leftover files from your computer.

About protection updates

Protection updates are files available from Symantec, by subscription, that keep your Symantec products up-to-date with the latest anti-threat technology. The protection updates you receive depend on which product you are using.

Norton AntiVirus, Norton SystemWorks	Users of Norton AntiVirus and Norton SystemWorks receive virus definition service updates, which provide access to the latest virus signatures and other technology from Symantec.
Norton Internet Security	In addition to the virus definition service, users of Norton Internet Security also receive protection updates to the Web filtering service, the intrusion detection service, and Spam Alert. The Web filtering service updates provide the latest lists of Web site addresses and Web site categories that are used to identify inappropriate Web content. The intrusion detection service updates provide the latest predefined firewall rules and updated lists of applications that access the Internet. These lists are used to identify unauthorized access attempts to your computer. Spam Alert updates provide the latest spam definitions and updated lists of spam email characteristics. These lists are used to identify unsolicited email.
Norton Personal Firewall	Users of Norton Personal Firewall receive intrusion detection service updates for the latest predefined firewall rules and updated lists of applications that access the Internet.

About your subscription

See "Subscription policy" on page 142.

Your Symantec product includes a complimentary, limited-time subscription to protection updates for the subscription services that are used by your product. When the subscription is due to expire, you are prompted to renew your subscription.

If you do not renew your subscription, you can still use LiveUpdate to obtain program updates. However, you cannot obtain protection updates and will not be protected against newly discovered threats.

When you should update

Run LiveUpdate as soon as you have installed your product. Once you know that your files are up-to-date, run LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

Request an update alert

To ensure your protection updates are current, you can request to receive an email alert whenever there is a high-level virus outbreak or other Internet security threat. The email alert describes the threat, provides detection and removal instructions, and includes advice on keeping your computer safe. You should always run LiveUpdate after you receive one of these alerts.

To request an update alert

1. From your Web browser, navigate to securityresponse.symantec.com/avcenter
2. On the Security Response Web page, scroll to the bottom of the page, then click **Symantec security response Free subscription**.
3. On the security alert subscription Web page, fill in the subscription form.
4. Click **Send me FREE Security Alerts**.

If you run LiveUpdate on an internal network

If you run LiveUpdate on a computer that is connected to a network that is behind a company firewall, your network administrator might set up an internal LiveUpdate server on the network. LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

If you can't use LiveUpdate

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can obtain new updates from the Symantec Web site.

Your subscription must be current to obtain new protection updates from the Symantec Web site.

To obtain updates from the Symantec Web site

1. Point your Web browser to securityresponse.symantec.com
2. Follow the links to obtain the type of update that you need.

Obtain updates using LiveUpdate

LiveUpdate checks for updates to all of the Symantec products that are installed on your computer.

If you connect to the Internet through America Online (AOL), CompuServe, or Prodigy, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.
   You might receive a warning that says that your subscription has expired. Follow the on-screen instructions to complete the subscription renewal.
3. In the LiveUpdate window, click **Next** to locate updates.
4. If updates are available, click **Next** to download and install them.
5. When the installation is complete, click **Finish**.

Some program updates may require that you restart your computer after you install them.

Set LiveUpdate to Interactive or Express mode

LiveUpdate runs in either Interactive or Express mode. In Interactive mode (the default), LiveUpdate downloads a list of updates available for your Symantec products that are supported by LiveUpdate technology. You can then choose which product updates you want to install. In Express mode,

LiveUpdate automatically installs all available updates for your Symantec products.

To set LiveUpdate to Interactive or Express mode

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.
3. On the LiveUpdate welcome screen, click **Configure**.
4. On the General tab of the LiveUpdate Configuration dialog box, select **Interactive Mode** or **Express Mode**.
5. If you selected Express Mode, select how you want to start checking for updates:
   - To have the option of cancelling the update, select **I want to press the start button to run LiveUpdate**.
   - To have any updates installed automatically whenever you start LiveUpdate, select **I want LiveUpdate to start automatically**.
6. Click **OK**.

Turn off Express mode

Once you have set LiveUpdate to run in Express mode, you can no longer access the LiveUpdate Configuration dialog box directly from LiveUpdate. You must use the Symantec LiveUpdate control panel.

To turn off Express mode

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. In the Control Panel window, double-click **Symantec LiveUpdate**.
3. On the General tab of the LiveUpdate Configuration dialog box, select **Interactive Mode**.
4. Click **OK**.

Run LiveUpdate automatically

You can have LiveUpdate check for protection updates automatically, on a set schedule, by enabling Automatic LiveUpdate. You must continue to run LiveUpdate manually to receive product updates.

Automatic LiveUpdate checks for an Internet connection every five minutes until a connection is found, and then every four hours. If you have an ISDN router that is set to automatically connect to your Internet service provider (ISP), many connections will be made, with connection and phone charges possibly being incurred for each connection. If this is a problem, you can set your ISDN router to not automatically connect to the ISP or disable Automatic LiveUpdate in the Norton Personal Firewall options.

To enable Automatic LiveUpdate

1. Start Norton Personal Firewall.
2. At the top of the Norton Personal Firewall main window, click **Options**.

   If you set a password for Options, Norton Personal Firewall asks you for the password before you can continue.
3. In the Norton Personal Firewall Options dialog box, on the LiveUpdate tab, check **Enable Automatic LiveUpdate**.
4. If you want to be notified when updates are available, check **Notify me when Norton Personal Firewall updates are available**.
5. Select the updates for which you want Automatic LiveUpdate to check.
6. For each type of update you want Automatic LiveUpdate to check for, set how you want those updates to be applied by selecting one of the following:

Automatically update my protection	LiveUpdate checks for and installs protection updates without prompting you. LiveUpdate displays an alert when a protection update has been downloaded. You should still run LiveUpdate occasionally to check for program updates.
Notify me	LiveUpdate checks for protection updates and asks if you want to install them.

7. Click **OK**.

To delete the schedule for Automatic LiveUpdate, disable Automatic LiveUpdate.

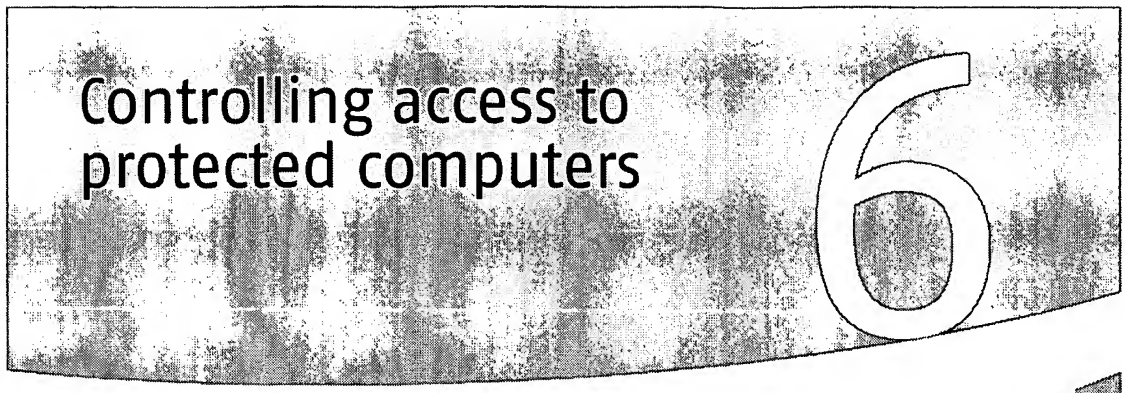
To disable Automatic LiveUpdate

1. Start Norton Personal Firewall.
2. At the top of the Norton Personal Firewall main window, click **Options**.

If you set a password for Options, Norton Personal Firewall asks you for the password before you can continue.

3. In the Norton Personal Firewall Options dialog box, click the **LiveUpdate** tab.
4. In the LiveUpdate pane, uncheck **Enable Automatic LiveUpdate**.
5. Click **OK**.

Controlling access to protected computers



You can configure Norton Personal Firewall to meet your needs in many different situations. You can use the program to control your computer's access to both local computers and computers over the Internet. You can also control how outside users access your computer.

Control how people use your computer

Norton Personal Firewall monitors all *connections*, including those made among computers in your home. After installation, you may need to adjust some settings to share files, printers, and other resources with other computers.

Connect to a network

Every time that you use Windows file sharing to exchange files with someone, print to a shared printer, or connect to the Internet using a *modem* or broadband connection, your computer joins a *network* of other computers. When you are part of a network, your computer is vulnerable to attacks. Norton Personal Firewall automatically monitors all new network connections to ensure that your computer is safe.

Normally, your computer connects to a network because of an action that you take. Unexpected connections can be a sign that a malicious program is attempting to send information over the Internet. Some wireless access cards automatically scan for and connect to any network in range. If you travel with a laptop that is equipped with a wireless access card, you may discover that your computer joins wireless networks in airports and other public places.

See "Monitoring Norton Personal Firewall" on page 103.

Whenever you join a network, Norton Personal Firewall automatically begins monitoring the connection. You do not need to make any changes in order to be protected. Norton Personal Firewall notifies you of the new connection and records it in the Connections *log*.

Enable file and printer sharing

Microsoft networking provides file and printer sharing. By default, Norton Personal Firewall prevents any computers from accessing these *services* on a protected computer.

To share files and give access to printers on your local *network*, you can enable file and printer sharing. If you enable these features on your local network, they are still protected from malicious users on the Internet.

Before enabling file and printer sharing on your local network, ensure that each shared resource is protected by a secure *password*. To learn more about securing shared resources, consult the Help file on your Start menu.

To enable file and printer sharing

1. Open Norton Personal Firewall.
2. In the Security Center, double-click **Personal Firewall**.
3. In the Personal Firewall window, on the Advanced tab, click **General Rules**.
4. In the General Rules window, select the entry for Windows file sharing or printer sharing.
5. Click **Modify**.
6. In the Modify Rule dialog box, on the Action tab, click **Permit Internet access**.
7. Click **OK**.
8. In the General Rules dialog box, click **OK**.
9. In the Advanced Firewall window, click **OK**.

Organize computers into network zones

Norton Personal Firewall lets you organize computers on your home network and the Internet into Trusted and Restricted Zones.

If you have more than one computer in your home, you will likely want to add all of these computers to your Trusted Zone. Only add external

computers to your Trusted Zone if you know that their users can be trusted and they have firewall software installed.

The Home Network Wizard is the fastest way to organize computers into zones. You can also manually add individual computers to zones.

To open the Home Network Wizard from the Security Center

1 Open Norton Personal Firewall.

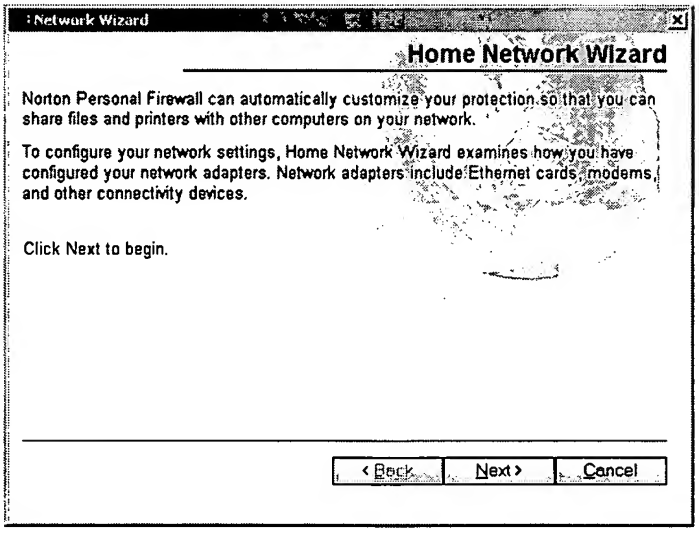
2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Home Networking tab, click **Wizard**.

To open the Home Network Wizard from the Security Monitor

1 Open Norton Personal Firewall.

2 In the Security Monitor, on the Select a Task menu, select **Setup Home Networking**.



To organize computers into zones with the Home Network Wizard

1 In the Home Network Wizard, click **Next**.

2 In the resulting list, check the network adapters that you want Norton Personal Firewall to configure automatically and add to your Trusted Zone.

3 Click **Next**.

4 Click **Finish** to close the wizard.

To manually add computers to zones

1. Open Norton Personal Firewall.
2. In the Security Center, double-click **Personal Firewall**.
3. In the Personal Firewall window, on the Home Networking tab, select the zone to which you want to add a computer.
4. Click **Add**.
5. In the Specify Computers window, identify the computer.
6. When you have finished adding computers, click **OK**.

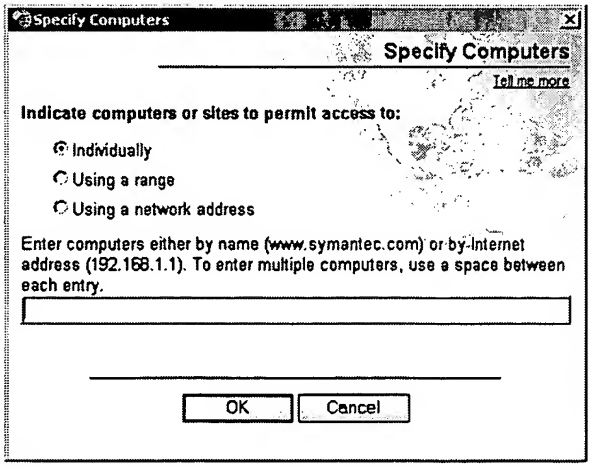
See "Identify computers to Norton Personal Firewall" on page 64.

To remove computers from zones

1. Open Norton Personal Firewall.
2. In the Security Center, double-click **Personal Firewall**.
3. Select the computer that you want to remove.
4. Click **Remove**.
5. When you have finished removing computers, click **OK**.

Identify computers to Norton Personal Firewall

You must identify computers to Norton Personal Firewall to manually configure network zones, firewall rules, and other protection features. In these cases, the Specify Computers dialog box appears.



The Specify Computers dialog box lets you specify computers in three ways. In each, you can use *IP addresses* to identify computers.

Find a computer's IP address

There are two procedures for finding a computer's IP address. On Windows 98/Me computers, you can use Winipcfg to find the IP address of a computer. On Windows 2000/XP computers, you can use Ipconfig to find the IP address of a computer.

To find an IP address with Winipcfg

1. On the Windows taskbar, click **Start** > **Run**.
2. In the Run dialog box, type **winipcfg**
3. Click **OK**.
4. Select the appropriate network adapter.
5. Record the IP address.

To find an IP address with Ipconfig

1. On the Windows taskbar, click **Start** > **Run**.
2. In the Run dialog box, type **cmd**
3. Click **OK**.
4. At the command prompt, type **ipconfig**
5. Click **OK**.
6. Record the IP address.

Specify an individual computer

The computer name that you type can be an IP address, a *URL* such as service.symantec.com, or a Microsoft Network computer name, such as Mojave. You can find the names of computers on your local network in Network Neighborhood or Network Places on your Windows desktop.

If you don't have TCP/IP bound to Client for Microsoft Networks in Windows Network Properties, you must use IP addresses instead of names for the computers on your local network.

To specify an individual computer

1. In the Specify Computers dialog box, click **Individually**.
2. Type the name or IP address of a single computer.
3. Click **OK**.

Specify a range of computers

You can enter a range of computers by specifying the starting (lowest numerically) IP address and the ending (highest numerically) IP address. All of the computers within that range of IP addresses are included.

In almost every case, the first three of the four numbers of the IP addresses entered should be the same.

To specify a range of computers

1. In the Specify Computers dialog box, click **Using a range**.
2. In the Starting Internet Address text box, type the starting (lowest numerically) IP address.
3. In the Ending Internet Address text box, type the ending (highest numerically) IP address.
4. Click **OK**.

Specify computers using a network address

You can identify all of the computers on a single *subnet* by specifying an IP address and a subnet mask. The IP address that you specify can be any address in the subnet that you are identifying.

To specify computers using a network address

1. In the Specify Computers dialog box, click **Using a network address**.
2. In the Network Address text box, type the IP address of a computer on the subnet.
3. In the Subnet Mask text box, type the subnet mask.
   The appropriate subnet mask is almost always 255.255.255.0.
4. Click **OK**.

If you use DHCP

If your *ISP* uses a *DHCP* server to provide IP addresses to users' computers, you must be careful when entering IP addresses.

Instead of identifying a computer with a single IP address, which might change at any time, enter a network address using a base IP address and a subnet mask. Enter values that cover the range of addresses that might be assigned to the computer.

Control how users access the Internet

Norton Personal Firewall supports most Internet *connection* methods without needing additional configuration.

If you access the Internet via a cable or DSL router

Norton Personal Firewall works behind a cable or DSL *router* and adds to the protection provided by the router. In some cases, you might want to reduce the protection provided by the router so that you can use programs like NetMeeting or Microsoft Messenger. Norton Personal Firewall also provides features that might not be available with cable and DSL routers, such as privacy protection.

If multiple computers share a single Internet connection

Norton Personal Firewall works with most Internet connection sharing programs. To protect your network from many outside attacks, install Norton Personal Firewall on the gateway computer. For maximum protection against *Trojan horses* or other problem programs that initiate *outbound connections*, install Norton Personal Firewall on all computers that share the connection.

Control how outside users access your network

Norton Personal Firewall can protect computers while still allowing outside users to access servers on your *network*. To run *servers* on protected computers, you may have to create firewall rules that let outside users connect to certain ports. For maximum security, only create these rules on the computers running your servers.

If you run Symantec pcAnywhere

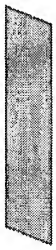
See "Change an existing firewall rule" on page 83.

You should have no problems using Symantec pcAnywhere as either a client or host with Norton Personal Firewall. For maximum protection, if you run a Symantec pcAnywhere host, edit the rule to limit its use to only the computers with which you use it. This, and Symantec pcAnywhere *passwords*, provide maximum security.

If you run a Virtual Private Network

Norton Personal Firewall works with the following Virtual Private Networks (VPNs):

- Nortel
- VPNRemote
- PGP
- SecureRemote



With most VPNs, when the VPN client is active, you cannot see the Internet or other computers on your local network. You can only see what is available through the VPN server to which you are connected.

Guarding against intrusion attempts 7

Internet attacks take advantage of the way that computers transfer information. Norton Personal Firewall can protect your computer by monitoring the information that comes into and out of your computer and blocking any attack attempts.

How Norton Personal Firewall protects against network attacks

Norton Personal Firewall includes three tools that protect your computer from intrusion attempts, malicious Web content, and *Trojan horses*:

- Norton Personal Firewall
  Monitors all Internet communication and creates a shield that blocks or limits attempts to view information on your computer
- Intrusion Detection
  Analyzes all incoming and outgoing information for data patterns typical of an attack
- Visual Tracking
  Identifies the computer responsible for the attack

Norton Personal Firewall monitors communications

When Norton Personal Firewall is active, it monitors communications among your computer and other computers on the Internet. It also protects your computer from such common security problems as:

Improper connection attempts	Warns you of any connection attempts from other computers and attempts by programs on your computer to connect to other computers
Trojan horses	Notifies you when your computer encounters destructive programs that are disguised as something useful
Security and privacy incursions by malicious Web content	Monitors all Java applets and ActiveX controls and lets you choose whether to run or block the program
Port scans	Cloaks inactive ports on your computer and detects port scans
Intrusions	Detects and blocks malicious traffic and attempts by outside users to attack your computer

See "Customize firewall protection" on page 72.

You can control the level of protection that Norton Personal Firewall provides by using the Security Level slider. You can also control how Norton Personal Firewall reacts to improper connection attempts, Trojan horses, and malicious Web content.

Intrusion Detection analyzes communications

Intrusion Detection scans each *packet* that enters and exits your computer for attack signatures, arrangements of information that identify an attacker's attempt to exploit a known operating system or program vulnerability.

Norton Personal Firewall protects your computer against most common Internet attacks, including the following.

Bonk	An attack on the Microsoft TCP/IP stack that can crash the attacked computer
RDS_Shell	A method of exploiting the Remote Data Services component of the Microsoft Data Access Components that lets a remote attacker run commands with system privileges
WinNuke	An exploit that can use NetBIOS to crash older Windows computers

Because attacks may span packets, Intrusion Detection examines packets in two different ways. It scans each packet individually looking for patterns that are typical of an attack. It also monitors the packets as a stream of information, which lets it identify attacks spread across multiple packets.

If the information matches a known attack, Intrusion Detection automatically discards the packet and severs the *connection* with the computer that sent the data. This protects your computer from being affected in any way.

You can modify how Intrusion Detection responds to attacks by excluding attack signatures from being monitored and by enabling or disabling AutoBlock, which automatically blocks all communication with an attacking computer. By excluding certain network behavior from blocking, you can continue to be productive, even while your computer is under attack.

Along with protecting your computer against attacks, Norton Personal Firewall also monitors all of the information that your computer sends to other computers. This ensures that your computer cannot be used to attack other users or be exploited by zombies.If Norton Personal Firewall detects that your computer is sending information that is typical of an attack, it immediately blocks the connection and warns you about the possible problem.

To reduce the number of warnings that you receive, Norton Personal Firewall only monitors attacks that are targeted at ports that your computer uses. If an attacker attempts to connect to your computer via an inactive port or a port that has been blocked by the firewall, Norton Personal Firewall will not notify you because there is no risk of an intrusion.

Norton Personal Firewall does not scan for intrusions by computers in your Trusted Zone. However, Intrusion Detection does monitor the information that you send to Trusted computers for signs of zombies and other remote control attacks.

See "Keeping current with LiveUpdate" on page 53.

Intrusion Detection relies on an extensive list of attack signatures to detect and block suspicious network activity. Run LiveUpdate regularly to ensure that your list of attack signatures is up to date.

Visual Tracking locates attackers

See "Identify the source of communications" on page 43.

Norton Personal Firewall now includes Visual Tracking, which lets you get information about the IP address used for a particular connection. This can help you identify the source of an attack.

Customize firewall protection

The default Norton Personal Firewall settings should provide adequate protection for most users. If the default protection is not appropriate, you can customize Norton Personal Firewall protection by using the Security Level slider to select preset security levels, or by changing individual security settings.

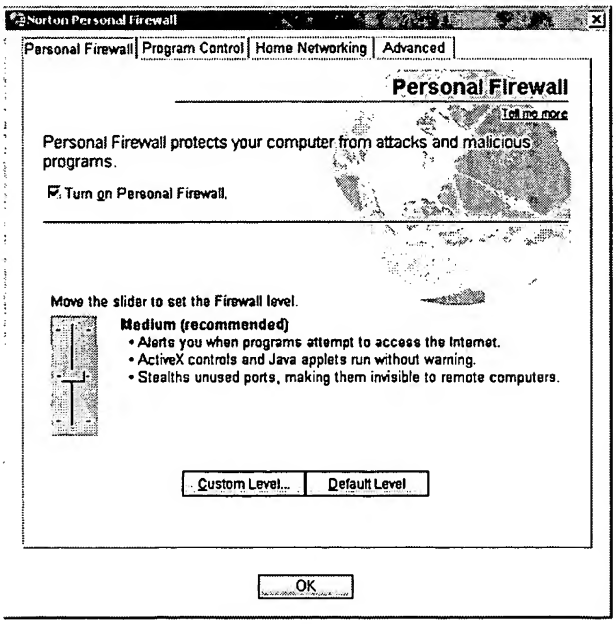
Change the Security Level slider

The Security Level slider lets you select Minimal, Medium, or High security settings. When you change the slider position, the protection level changes. Changing the Security Level slider does not affect the protection provided by Intrusion Detection.

To change the Security Level slider

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.



3 Move the slider to the Security Level that you want. Your options are:

High	The firewall blocks everything until you allow it. If you have run a Program Scan, you should not be interrupted frequently with Program Control alerts. See "Enable Automatic Program Control" on page 76. You are alerted each time that an ActiveX control or Java applet is encountered. Unused ports do not respond to connection attempts, giving them a stealth appearance.
Medium (recommended)	The firewall blocks everything until you allow it. If you have run a Program Scan, you should not be interrupted frequently with Program Control alerts. ActiveX controls and Java applets run without warning. Unused ports do not respond to connection attempts, giving them a stealth appearance.
Minimal	Firewall blocks connection attempts by Trojan horse programs. ActiveX controls and Java applets run without warning.

Change individual security settings

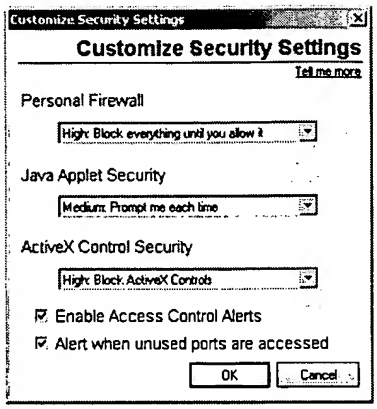
If the Security Level options do not meet your needs, you can change the settings for Norton Personal Firewall, *Java*, and *ActiveX* protection levels. Changing an individual setting overrides the Security Level, but it does not change the other security settings in that level.

To change individual security settings

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.

3 Click **Custom Level**.



4 Do one or more of the following:

- On the Personal Firewall menu, select a level. Your options are:

High	Blocks all communication that you do not specifically allow. You must create firewall rules for every program that requests Internet access.
Medium	Blocks many ports that are used by harmful programs. However, it can also block useful programs when they use the same ports.
None	Disables Norton Personal Firewall and allows all Internet communications.

- On the Java Applet Security or ActiveX Control Security menu, select a level. Your options are:

High	Blocks your browser from running any Java applets or ActiveX controls over the Internet. This is the safest, but most inconvenient, option. Some Web sites might not operate properly using this setting.
Medium	Prompts you when Java applets and ActiveX controls are encountered. This lets you temporarily or permanently allow or block each Java applet or ActiveX control that you encounter. It can be bothersome to respond every time that you encounter a Java applet or ActiveX control, but it lets you decide which ones to run.
None	Lets Java applets and ActiveX controls run whenever you encounter them.

- To be notified whenever unknown programs access the Internet, check **Enable Access Control Alerts**.
- To be notified whenever a remote computer attempts to connect to a port no program is using, check **Alert when unused ports are accessed**.

5 Click **OK**.

Reset security settings to defaults

Setting a custom security level disables the Security Level slider. The slider indicates the security level on which your custom level is based, but you cannot use the slider to make changes to your settings. To use the slider to choose a preset security level, you must reset the security level.

To reset security settings to defaults

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.

3 Click **Default Level**.

This resets your security level to medium. Use the Security Level slider to choose one of the other preset security levels.

See "Change the Security Level slider" on page 72.

Customize firewall rules

Firewall rules control how Norton Personal Firewall protects your computer from malicious incoming traffic, programs, and *Trojan horses*. The firewall automatically checks all data coming in or out of your computer against these rules.

How firewall rules are processed

When a computer attempts to connect to your computer, or when your computer attempts to connect to a computer on the Internet, Norton Personal Firewall compares the type of *connection* with its list of firewall rules.

Firewall rules are processed in a set order based on their types. System rules are processed first, followed by program rules, and then Trojan horse rules.

Once a rule that blocks or permits communications is matched, all remaining rules are ignored. In other words, additional rules that match

this type of communication are ignored if they appear below the first rule that matches.

If no matching rule is found, the communication is blocked. Depending on the Reporting level, an alert may appear.

Create new firewall rules

Norton Personal Firewall includes Program Control, which helps you create firewall rules as you use the Internet.

There are four ways to create firewall rules with Program Control:

Enable Automatic Program Control	Automatically configures access for well-known programs the first time that users run them. This is the easiest way to set up firewall rules.
Use Program Scan	Finds and configures access for all Internet-enabled programs on a computer at once.
Manually add programs	Closely manage the list of programs that can access the Internet.
Respond to alerts	Norton Personal Firewall warns users when a program attempts to access the Internet for the first time. Users can then allow or block Internet access for the program.

Enable Automatic Program Control

When Automatic Program Control is active, Norton Personal Firewall can automatically configure Internet access settings for programs the first time that they run. Automatic Program Control only configures Internet access for the versions of programs that Symantec has identified as safe.

If an unknown program or an unknown version of a known program attempts to access the Internet, Norton Personal Firewall warns the user. The user can then choose to allow or block Internet access for the program.

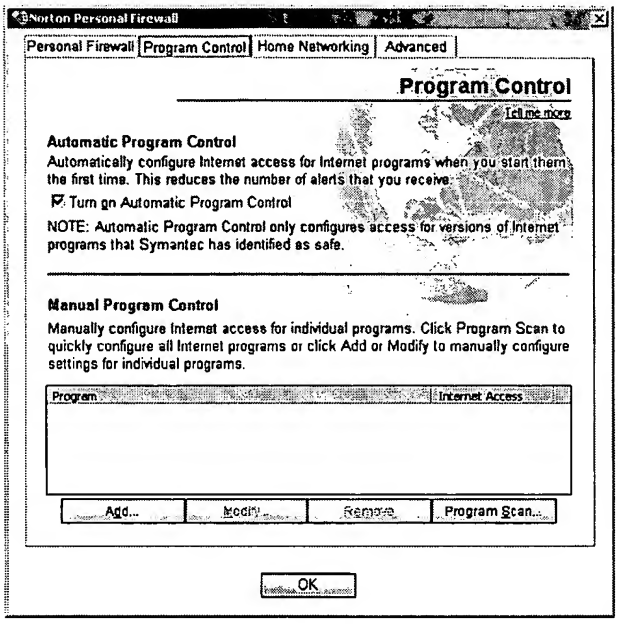
See "Keeping current with LiveUpdate" on page 53.

Symantec regularly updates the list of recognized programs. You should run LiveUpdate regularly to ensure that your list is up-to-date.

To enable Automatic Program Control

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.



3 In the Personal Firewall window, on the Program Control tab, check **Turn on Automatic Program Control**.

4 Click **OK**.

Scan for Internet-enabled programs

Scanning for Internet-enabled programs is the quickest way to configure the Personal Firewall. Norton Personal Firewall scans the computer for programs that it recognizes and suggests appropriate settings for each program.

You can scan for Internet-enabled programs from the Security Center or the Security Monitor.

To scan for Internet-enabled programs from the Security Center

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Program Control tab, click **Program Scan**.

4 Select the disk or disks on your computer that you want to scan.

5 Click **OK**.

6 In the Program Scan window, do one of the following:

- Check programs that you want to add to the Program Control list.
- To add all Internet-enabled programs at once, click **Check All**.

7 Click **Finish**.

8 Click **OK**.

To scan for Internet-enabled programs from the Security Monitor

1 Open Norton Personal Firewall.

2 In the Security Monitor, on the Select a Task menu, click **Program Scan**.

3 Select the disk or disks on your computer that you want to scan.

4 Click **OK**.

5 In the Program Scan window, do one of the following:

- Check programs that you want to add to the Program Control list.
- To add all Internet-enabled programs at once, click **Check All**.

6 Click **Finish**.

Manually add a program to Program Control

See "Customize firewall protection" on page 72.

Users can add programs to Program Control to strictly control the programs' ability to access the Internet. This overrides any settings made by Automatic Program Control.

To add a program to Program Control

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Program Control tab, click **Add**.

4 Select the program's executable file.
Executable file names typically end in .exe.

5 Click **Open**.

6 In the Internet Access Control alert, select the access level you want this program to have. Your options are:

Automatically configure Internet access (Recommended)	Use the default Norton Personal Firewall settings for this program.
Permit	Allow all access attempts by this program.
Block	Deny all access attempts by this program.
Manually configure Internet Access	Create rules controlling how this program accesses the Internet.

7 If you want to see any risks that this program could pose to your computer, click **Details**.

8 Click **OK**.

Change Program Control settings

After using Norton Personal Firewall for a while, you may find that you need to change access settings for certain programs. Any changes override settings made by Automatic Program Control.

To change Program Control settings

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Program Control tab, in the list of programs, click the program that you want to change.

4 Click **Modify**.

5 In the Internet Access Control alert, select the access level you want this program to have. Your options are:

Automatically configure Internet access	Use the default Norton Personal Firewall settings for this program.
Permit this program access to the Internet	Allow all access attempts by this program.
Block this program from accessing the Internet	Deny all access attempts by this program.
Customize Internet access for this program	Create rules controlling how this program accesses the Internet.

6 Click **OK**.

Manually add a firewall rule

While Norton Personal Firewall automatically creates most of the firewall rules that you need, you may want to add specific rules. Only experienced Internet users should create their own firewall rules.

There are three sets of firewall rules you can customize:

- General Rules
- Trojan Horse Rules
- Program Rules

To add a General Rule

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Advanced tab, click **General Rules**.

4 Follow the on-screen instructions.
See "Write a firewall rule" on page 81.

To add a Trojan Horse Rule

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Advanced tab, click **Trojan Horse Rules**.

4 Follow the on-screen instructions.
See "Write a firewall rule" on page 81.

To add a Program Rule

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Program Control tab, in the list of programs, click **Add**.

4 In the Select a program window, select a program's executable file. Executable file names typically end in .exe.

5 In the Internet Access Control alert, on the What do you want to do menu, select **Create a firewall rule**.

6 Follow the on-screen instructions.
See "Write a firewall rule" on page 81.

Write a firewall rule

Norton Personal Firewall leads you through the process of writing your own firewall rules.

To write a firewall rule

1 In the General Rules, Trojan Horse Rules, or Program Rules window, click **Add**.

2 In the Add Rule window, select the action that you want for this rule. Your options are:

Permit Internet Access	Allows communication of this type to take place.
Block Internet Access	Prevents communication of this type from taking place.
Monitor Internet Access	Updates the Firewall tab in the Event Log or shows a message each time that communication of this type takes place. This lets you monitor how often this firewall rule is used. To monitor a permitted connection, you must create both a monitor and a permit rule. The monitor rule must precede the permit rule.

3 Click **Next**.

4 Select the type of connection the rule should monitor. Your options are:

Connections to other computers	The rule applies to outbound connections from your computer to another computer.
Connections from other computers	The rule applies to inbound connections from another computer to your computer.
Connections to and from other computers	The rule applies to both inbound and outbound connections.

5 Click **Next**.

6 Select the computers the rule should monitor. Your options are:

Any computer	The rule applies to all computers.
Only computers specified below	The rule applies only to the computers, sites, and domains listed.
Adapters	The rule applies to a specific network adapter in your computer. This allows you to customize firewall rules for each of your computer's IP addresses. For example, if your computer is connected to a home network and to the Internet, you might want to set up a rule that permits file sharing on the home network, while another rule blocks file sharing over the Internet.

7 Click **Next**.

8 Select the protocols the rule should monitor. Your options are:

TCP	The rule applies to TCP (Transmission Control Protocol) communications.
UDP	The rule applies to UDP (User Datagram Protocol) communications.
TCP and UDP	The rule applies to both TCP and UDP communications.
ICMP	The rule applies to ICMP (Internet Control Message Protocol) communications. This option is only available when adding or modifying a General Rule.

9 Select the ports the rule should monitor. Your options are:

All types of communications (all ports)	The rule applies to communications using any port.
Only the types of communications or ports listed below	The rule applies to the ports listed. You can add ports to, or remove ports from, the list.

10 Click **Next**.

11 Choose if and how you want Norton Personal Firewall to track this rule. Your options are:

Do not track this rule	No record of the actions of this rule is made.
Create an Event Log entry	An entry is created in the firewall Event Log when a network communication event matches this rule.
Notify me with an Alert Tracker message	An Alert Tracker message appears when a network communication event matches this rule.
Display Security Alert	A Security Alert dialog box appears when a network communication event matches this rule.

12 Click **Next**.

13 In the **What do you want to call this rule?** text box, type a name for this rule.

14 Click **Next**.

15 Review the new rule settings, then click **Finish**.

16 When you have finished adding rules, click **OK**.

Change an existing firewall rule

You can change firewall rules if they are not functioning the way that you want.

To change an existing firewall rule

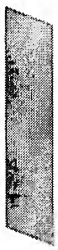
1. In the General Rules, Trojan Horse Rules, or Program Rules window, click **Add**.
2. Select the rule that you want to change.
3. Click **Modify**.
4. Follow the on-screen instructions to change any aspect of the rule.
5. When you have finished changing rules, click **OK**.

See "Write a firewall rule" on page 81.

Change the order of firewall rules

Norton Personal Firewall processes each list of firewall rules from the top down. You can determine how Norton Personal Firewall processes firewall rules by changing their order.

See "How firewall rules are processed" on page 75.



To change the order of a firewall rule

1. In the General Rules, Trojan Horse Rules, or Program Rules window, select the rule that you want to move.
2. Do one of the following:
   - To have Norton Personal Firewall process this rule before the rule above it, click **Move Up**.
   - To have Norton Personal Firewall process this rule after the rule below it, click **Move Down**.
3. When you are done moving rules, click **OK**.

Temporarily disable a firewall rule

You can temporarily disable a firewall rule if you need to allow specific access to a computer or program.

To temporarily disable a firewall rule

- In the General Rules, Trojan Horse Rules, or Program Rules window, uncheck the box next to the rule you want to disable.

Remember to re-enable the rule when you are done working with the program or computer that required the change.

Remove a firewall rule

Remove firewall rules when they are no longer necessary.

To remove a firewall rule

1. In the General Rules, Trojan Horse Rules, or Program Rules window, click **Add**.
2. Select the rule that you want to remove.
3. Click **Remove**.
4. When you are done removing rules, click **OK**.

Reset firewall rules to the default settings

Resetting the firewall rules returns the firewall to its default settings and deletes any changes you have made to firewall rules.

You should only use this procedure in an emergency. Before resetting your firewall rules, try removing recently changed firewall rules.

To reset the firewall rules to the default settings

1. Close all Norton Personal Firewall windows.
2. In Windows Explorer, double-click **My Computer**.
3. Double-click the hard disk on which you installed Norton Personal Firewall.
   In most cases, this will be drive C.
4. Open **Program Files > Common Files > Symantec Shared**.
5. Drag **firewall.rul** to the Recycle Bin.

The firewall will return to its default settings the next time you run Norton Personal Firewall.

Customize Intrusion Detection

The default Intrusion Detection settings should provide adequate protection for most users. You can customize Intrusion Detection by excluding specific network activity from monitoring, enabling or disabling AutoBlock, and restricting blocked computers.

Exclude specific network activity from being monitored

In some cases, benign network activity may appear similar to a Norton Personal Firewall attack signature. If you receive repeated warnings about possible attacks, and you know that these attacks are being triggered by

safe behavior, you can create an exclusion for the attack signature that matches the benign activity.

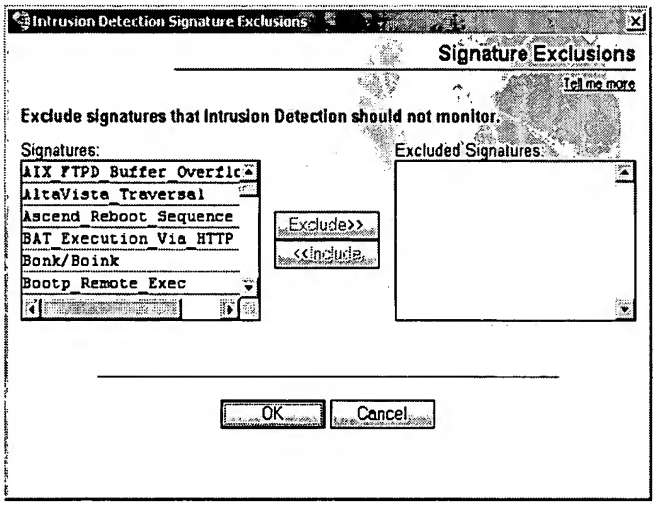
Each exclusion that you create leaves your computer vulnerable to attacks. Be very selective when excluding attacks. Only exclude behavior that is always benign.

To exclude attack signatures from being monitored

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Intrusion Detection**.

3 In the Intrusion Detection window, click **Signatures**.



4 In the Signatures list, select the attack signature that you want to exclude.

5 Click **Exclude**.

6 When you are done excluding signatures, click **OK**.

If you have excluded attack signatures that you want to monitor again, you can include them in the list of active signatures.

To include attack signatures

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Intrusion Detection**.

3 In the Intrusion Detection window, click **Signatures**.

4 In the Excluded Signatures list, select the attack signature that you want to monitor.

5 Click **Include**.

6 When you are done including signatures, click **OK**.

Enable or disable AutoBlock

When Norton Personal Firewall detects an attack, it automatically blocks the *connection* to ensure that your computer is safe. The program can also activate AutoBlock, which automatically blocks all incoming communication from the attacking computer for a set period of time, even if the incoming communication does not match an attack signature.

AutoBlock stops all inbound communications with the attacking computer for 30 minutes.

To enable or disable AutoBlock

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Intrusion Detection**.

3 In the Intrusion Detection window, check or uncheck **Turn on AutoBlock**.

Unblock computers

If a computer that you need to access appears on the list of computers currently blocked by AutoBlock, unblock it. If you have changed your protection settings and want to reset your AutoBlock list, you can unblock all of the computers on the AutoBlock list at once.

To unblock computers currently blocked by AutoBlock

1 Open Norton Personal Firewall.

2 In the Security Center, double-click **Intrusion Detection**.

3 In the Intrusion Detection window, do one of the following:

- To unblock one computer, select its IP address, then click **Unblock**.
- To unblock all computers on the AutoBlock list, click **Unblock All**.

Exclude computers from AutoBlock

If a computer you need to access is repeatedly placed in the AutoBlock list, you can exclude it from being blocked by AutoBlock.

To exclude specific computers from AutoBlock

1. Open Norton Personal Firewall.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the Intrusion Detection window, click **IP Address**.
4. Do one of the following:
   - In the Currently blocked list, select a blocked IP address, then click **Exclude**.
   - Click **Add**, then type the computer's name, IP address, network identification, or a range of IP addresses containing the computer that you want to exclude.
5. When you are done excluding IP addresses, click **OK**.

Restrict a blocked computer

You can add a blocked computer to your Restricted Zone to permanently prevent that computer from accessing your computer. Computers added to the Restricted Zone do not appear on the blocked list because Norton Personal Firewall automatically rejects any *connection attempts* by restricted computers.

To restrict a blocked computer

1. Open Norton Personal Firewall.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the list of computers that are currently blocked by AutoBlock, select the computer to add to the Restricted Zone.
4. Click **Restrict**.
5. When you are done restricting computers, click **OK**.

Protecting your privacy

8

Every time that you browse the Internet, computers and *Web sites* collect information about you. Some of this information comes from forms that you fill out and choices that you make. Other information comes from your *browser*, which automatically provides information about the Web page you last visited and the type of computer that you're using.

Malicious users can also collect personal information without your knowledge. Any time that you send information over the Internet, the data must pass through a number of computers before it reaches its destination. During transmission, it's possible for third parties to intercept this information.

Computers include some basic security features, but they might not be enough to protect your personal information. Privacy Control helps protect your privacy by giving you several levels of control over *cookies* and other information that your browser sends to Web sites.

Privacy Control can ensure that users don't send private information, such as credit card numbers, over the Internet unless they are encrypted, or you specifically allow it.

Identify private information to protect

Many *Web sites* ask for your name, *email* address, and other personal information. While it is generally safe to provide this information to large, reputable sites, malicious sites can use this information to invade your privacy. It is also possible for people to intercept information sent via the Web, email, and instant messenger programs.

Privacy Control lets you create a list of information that you want to remain private. If someone attempts to send protected information over the Internet, Norton Personal Firewall warns them about the security risk or blocks the *connection*.

Privacy Control and SSL

Some Web sites and email servers use SSL (Secure Sockets Layer) connections to encrypt connections between your computer and the server. Privacy Control cannot block private information sent via SSL connections. However, since the information is encrypted, only the recipient of the email will be able to read the message.

Add private information

You must add information that you want to protect to the Norton Personal Firewall Private Information list.

To add private information

1. Start Norton Personal Firewall.
2. Do one of the following:
   - In the Security Center, double-click **Privacy Control**, then click **Private Information**.
   - In the Security Monitor, on the Select a Task menu, click **Edit Private Information**.
3. In the Private Information dialog box, click **Add**.
4. In the Add Private Information dialog box, under Type Of Information To Protect, select a category.
5. In the Descriptive Name text box, type a description to help you remember why you are protecting this information.
6. In the Information To Protect text box, type the information that you want to block from being sent over nonsecure Internet connections.
7. Under Secure this private information in, select the Internet programs in which Privacy Control should block this information:
   - Web browsers
   - Instant messengers
   - Email programs
8. Click **OK**.

Modify or remove private information

You can modify or remove private information at any time.

To modify or remove private information

1. Start Norton Personal Firewall.
2. In the Security Center, double-click **Privacy Control**.
3. In the Privacy Control window, click **Private Information**.
4. Select the private information that you want to change or remove.
5. Select one of the following:
   - Modify
   - Remove
6. Click **OK**.

Customize Privacy Control

Privacy Control protects four areas:

Private Information	Blocks specific strings of text that you do not want sent over the Internet
Cookie Blocking	Stops Web sites from retrieving personal information stored in cookie files
Browser Privacy	Protects information about your browsing habits
Secure Connections	Prevents users from establishing secure connections to online stores and other Web sites

There are two ways to adjust Privacy Control settings:

- Set the Privacy Level
  Use the slider in the main Privacy Control pane to select pre-set security levels.
- Adjust individual Privacy Control settings
  Customize your protection by manually adjusting individual settings.

Set the Privacy Level

Norton Personal Firewall offers pre-set security levels that help you set several Privacy Control options at one time. The Privacy Level slider lets you select minimal, medium, or high protection.

To set the Privacy Level

1 Start Norton Personal Firewall.

2 Double-click **Privacy Control**.

3 Move the slider to the Privacy Level that you want. Your options are:

High	All personal information is blocked and an alert appears each time that a cookie is encountered.
Medium (recommended)	An alert appears if private information is typed into a Web form or instant messenger program. Conceals your browsing from Web sites. Cookies are not blocked.
Minimal	Confidential information is not blocked. Cookies are not blocked. Conceals your browsing from Web sites.

4 Click **OK**.

Adjust individual Privacy Control settings

You can change the settings for Private Information, Cookie Blocking, Browser Privacy, and Secure Connections if the Privacy Level settings do not meet your needs. For example, you can choose to block all attempts to send private information while allowing Web sites to customize their pages using your browser information.

Change the Private Information setting

Change the Private Information setting to control how Norton Personal Firewall handles attempts to send information on the Private Information list over the Internet.

To change the Private Information setting

1 Start Norton Personal Firewall.

2 Double-click **Privacy Control**.

3 Click **Custom Level**.

4 Select the Private Information setting that you want. Your options are:

High	Blocks all private information
Medium	Alerts you each time that you attempt to send private information to a nonsecure Web site or through an instant messenger program
None	Does not block private information

5 Click **OK**.

Change the Cookie Blocking setting

Many Web sites store information they collect in *cookies* placed on your hard disk. When you return to a site that has set a cookie on your computer, the Web server opens and reads the cookie.

Most cookies are harmless. Sites use them to personalize Web pages, remember choices that you have made on the site, and deliver optimized pages for your computer. However, sites can also use cookies to track your Internet usage and browsing habits.

Change the Cookie Blocking setting to control how Norton Personal Firewall handles sites that attempt to place cookies on your computer.

To change the Cookie Blocking setting

1 Start Norton Personal Firewall.

2 Double-click **Privacy Control**.

3 Click **Custom Level**.

4 Select the Cookie Blocking setting that you want. You have three options:

High	Blocks all cookies
Medium	Alerts you each time that a cookie is encountered
None	Allows cookies

5 Click **OK**.

Enable or disable Browser Privacy

Browser Privacy prevents Web sites from learning the type of *browser* that you are using, the Web site that you last visited, and other information about your browsing habits. Some Web sites that depend on JavaScript may not work correctly if they cannot identify the type of browser that you are using.

To enable or disable Browser Privacy

1. Start Norton Personal Firewall.
2. Double-click **Privacy Control**.
3. Click **Custom Level**.
4. In the Customize Privacy Settings dialog box, check or uncheck **Enable Browser Privacy**.
5. Click **OK**.

Disable or enable secure Web connections

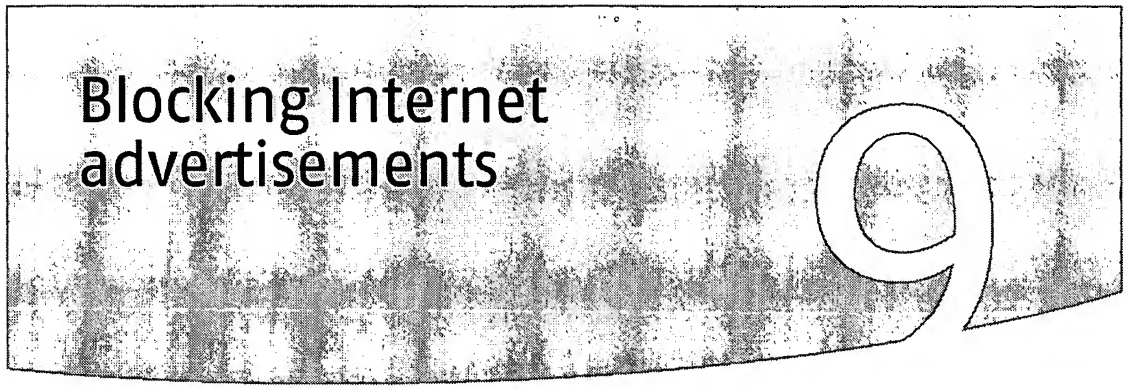
When you visit a secure Web site, your browser sets up an encrypted *connection* with the Web site. By default, Norton Personal Firewall lets any account use secure connections. If you want to ensure that users are not sending private information to secure Web sites, you can disable secure Web connections.

If you disable secure Web connections, your browser will not encrypt any information that it sends. You should only disable secure Web connections if you are protecting your personal data in the Private Information list.

To disable or enable secure Web connections

1. Start Norton Personal Firewall.
2. Double-click **Privacy Control**.
3. Click **Custom Level**.
4. In the Customize Privacy Settings dialog box, check or uncheck **Enable Secure Connections (https)**.
5. Click **OK**.

Blocking Internet advertisements



Many Web sites are using more aggressive techniques to draw attention to the ads on their pages. Some have begun using larger, more prominent ads, while others rely on ad windows that appear when you enter or leave the site. Along with increasing the amount of time that it takes to display Web pages, some ads contain offensive content, cause software conflicts, or use *HTML* tricks to open additional *browser* windows.

Ad Blocking helps avoid these problems. When Ad Blocking is active, Norton Personal Firewall transparently removes:

- Ad banners
- Pop-up and pop-under ads
- Macromedia Flash-based ads

How Ad Blocking works

Norton Personal Firewall detects and blocks ads based on two criteria: their dimensions and their locations.

Blocking by dimensions

Most online advertisers use one or more standard sizes for their ads. Norton Personal Firewall now includes the ability to block images, Flash animations, and other *HTML* elements that have the same dimensions as these common ad sizes.

Blocking by location

Every file on the Internet has a unique address or *URL*. When you view a Web page, your computer connects to a URL and displays the file that is stored there. If the page points to graphics, audio files, and other multimedia content, your *browser* displays the files as part of the page.

When you go to a Web page that includes a *banner ad*, the instructions used to display the page might include the following:

<p>Greetings from the Ajax company<img src="http://www.ajax.com/nifty_images/image7.gif">

Your browser displays the text Greetings from the Ajax company on the screen. Then it connects to www.ajax.com and requests a file called /nifty_images/image7.gif. (The suffix .gif indicates that this is a Graphics Interchange Format file, a common image file format.) The computer at www.ajax.com sends the file to the browser, which displays the image.

When Ad Blocking is enabled and you connect to a Web site, Norton Personal Firewall scans Web pages and compares their contents to two lists:

See "Keeping current with LiveUpdate" on page 53.

- A default list of ads that Norton Personal Firewall blocks automatically. Use LiveUpdate to keep the list of blocked ads current.
- A list that you create as you block specific ads. You can add to and change this list.

If the page includes files from a blocked *domain*, Norton Personal Firewall removes the link and downloads the rest of the page.

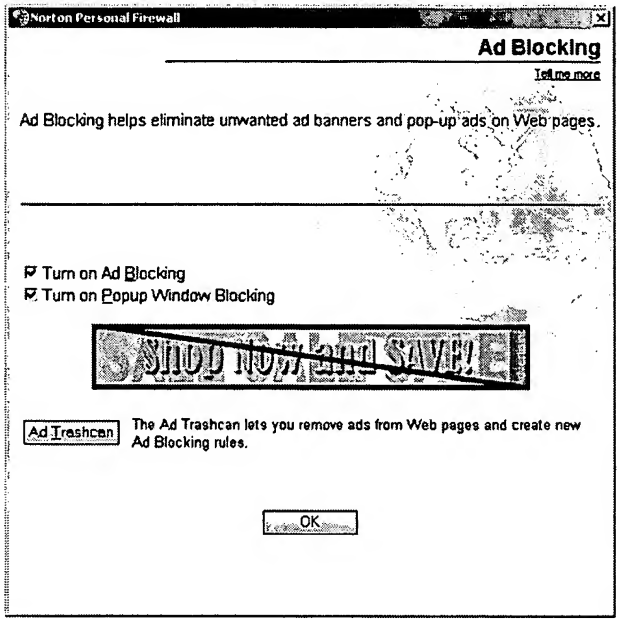
Enable or disable Ad Blocking

Norton Personal Firewall searches for the addresses of the ads that are being blocked as the Web page is downloaded by your *browser*. If it finds an address that matches the list of ads to block, it removes the ad so that it does not appear in your browser. It leaves the rest of the Web page intact so that you can view the page without the advertisements.

To enable or disable Ad Blocking

1 Open Norton Personal Firewall.

2 Double-click **Ad Blocking**.



3 Check or uncheck **Turn on Ad Blocking**.

4 Click **OK**.

Enable or disable Popup Window Blocking

Pop-up and pop-under ads are secondary windows that Web sites open when you visit or leave the sites. Pop-ups appear on top of the current window, while pop-unders appear behind the current window.

When Popup Window Blocking is active, Norton Personal Firewall automatically blocks the programming code Web sites use to open secondary windows without your knowledge. Sites that open secondary windows when you click a link or perform other actions are not affected.

To enable or disable Popup Window Blocking

1 Open Norton Personal Firewall.

2 Double-click **Ad Blocking**.

3 Check or uncheck **Turn on Popup Window Blocking**.

4 Click **OK**.

Enable or disable Flash blocking

When Ad Blocking is active, Norton Personal Firewall automatically blocks all Flash animations that have the same dimensions as common ads. Norton Personal Firewall can also block all Flash content. This is useful if you have a slow connection or are not interested in viewing Flash animations.

You can choose to have Norton Personal Firewall block all Flash animations or only block them on certain Web sites.

To enable or disable Flash blocking

1. Open Norton Personal Firewall.
2. In the Security Center, click **Options** > **Internet Security**.
3. On the Web Content tab, click the **Global Settings** tab.
4. In the list of Web sites, do one of the following:
   - To change Flash settings for all sites, click **(Defaults)**.
   - To change Flash settings for a site in the list, click the site's name.
   - To change Flash settings for a site not in the list, click **Add Site**, then in the New Site/Domain dialog box, type the site's address.
5. In the Flash animation section, select one of the following:
   - Block
   - Permit
6. Click **OK**.

Some Web sites use Flash to create navigation toolbars. Blocking Flash may make these sites unusable.

Use the Ad Trashcan

As you use the Internet, you may find ads that are not included on the default Norton Personal Firewall Ad Blocking list. You can use the Ad Trashcan to add these to your personal list of blocked ads.

To use the Ad Trashcan

1. Open your Web browser and view the page containing the advertisement that you want to block.
2. Open Norton Personal Firewall.

3 In the Security Center, double-click **Ad Blocking**.

4 In the Ad Blocking window, ensure that Enable Ad Blocking is checked.

5 Click **Open the Ad Trashcan**.
The Ad Trashcan window appears.

6 With the windows arranged so that you can see both the advertisement and the Ad Trashcan window, do one of the following:
- If you are using Microsoft Internet Explorer, drag the unwanted ad from the Web site to the Ad Blocking dialog box.
- If you are using Netscape, right-click the advertisement, then click **Copy Image Location**. In the Ad Trashcan, click **Paste**. The address for the advertisement appears in the Ad Details line of the Ad Trashcan dialog box.

7 Select one of the following:
- Add: Block this address.
- Modify: Change the entry before adding it to the Ad Blocking list. For example, if the advertisement address is http://www.advertise.org/annoying/ads/numberone.gif, you could change it to http://www.advertise.org/annoying/ads/ to block everything in the ads directory.

8 Click **OK**.

Use text strings to identify ads to block or permit

You can control whether Norton Personal Firewall displays specific ads by creating a list of text strings that identify individual ad banners. Ad Blocking strings are sections of *HTML* addresses. If any part of a file's address matches the text string, Norton Personal Firewall automatically blocks the file.

Norton Personal Firewall provides a predefined (Defaults) Ad Blocking list that is used to determine which images should be blocked when displaying Web pages.

When Ad Blocking is enabled, all Web pages are scanned for the HTML strings specified in the (Defaults) list. Norton Personal Firewall looks for the blocked strings within HTML tags that are used to present advertising. The HTML structures that contain matching strings are removed from the page by Norton Personal Firewall before the page appears in the Web *browser*.

Make sure that what you place in the (Defaults) block list isn't too general. For example, www by itself is not a good string to block because almost every *URL* includes www. A string like www.slowads is more effective because it only blocks graphics from the slowads *domains* without affecting other sites.

How to identify Ad Blocking strings

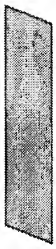
The way that you define Ad Blocking strings affects how restrictive or unrestrictive Norton Personal Firewall is when filtering data.

For example, if you add the string ajax.com to the (Defaults) block list, you block everything in the ajax.com domain. If you are more specific and add the string nifty_images/image7.gif to the site-specific block list maintained for www.ajax.com, you block only that particular image.

Blocking all images on a particular site may make that site unusable. A good compromise is to block only the directories that contain ads. For example, if www.ajax.com stores its ads in /nifty_images/ and its navigational images in /useful_images/, you could block www.ajax.com/nifty_images/ without seriously impeding your ability to use the site.

You can also create permit strings that allow Web sites to display images that match the string. This allows you to override the blocking effect of any string in the (Defaults) block list for individual sites. Permit rules take precedence over Block rules on any site.

Add an Ad Blocking string



You can add strings to the Ad Blocking list for all sites or for individual sites.

To add an Ad Blocking string

1. Open Norton Personal Firewall.
2. At the top of the Security Center window, click **Options > Internet Security**.
3. On the Web Content tab, on the Ad Blocking tab, do one of the following:
   - To block a string on all Web sites, click **(Defaults)**.
   - To block a string on a Web site in the list, select the site's name.
   - To block a string on a Web site not in the list, click **Add Site**, then in the New Site/Domain dialog box, type the site's address.

4 On the Ad Blocking tab, click **Add**.

5 In the Add New HTML String dialog box, select the action that you want to take. Your options are:

Block	Block ads matching this string.
Permit	Allow ads matching this string.

6 Type an HTML string to block or permit.

7 Click **OK**.

Modify or remove an Ad Blocking string

If you later decide that an Ad Blocking string is too restrictive, not broad enough, or not appropriate, you can change or remove it.

To modify or remove an Ad Blocking string

1 Open Norton Personal Firewall.

2 At the top of the Security Center window, click **Options > Internet Security**.

3 On the Web Content tab, on the Ad Blocking tab, do one of the following:

- To modify or remove a string in the (Defaults) list, click **(Defaults)**.
- To modify or remove a site-specific string, click the site's name.

4 In the HTML string list, select the string that you want to change.

5 Do one of the following:

- To modify a string, click **Modify**, then type your changes.
- To remove a string, click **Remove**.

6 Click **OK**.

Monitoring Norton Personal Firewall 10

Norton Personal Firewall maintains records of every ingoing and outgoing Internet *connection* and any actions that the program takes to protect your computer. You should periodically review this information to spot potential problems.

There are four sources of Norton Personal Firewall information:

Status & Settings window	Basic information about which protection features are active
Statistics window	Recent information about firewall and content-blocking activities
Detailed statistics window	Detailed information about network activity and actions that Norton Personal Firewall has taken
Event Log	Internet activities and any actions Norton Personal Firewall has taken

When reviewing logged information, check for:

- Recent attacks in the Status & Settings window
- Many denied accesses, especially from a single *IP address*
- Sequences of *port numbers* from the same IP address, possibly indicating a *port scan*
- Excessive network activity by unknown programs

It is normal to see some denied access attempts on a random basis (not all from the same IP address, and not to a sequence of port numbers). You may also see logged access attempts made due to activity on your own computer such as connecting to an FTP server and sending *email* messages.

If you see any of the above patterns, it could be evidence of an attack.

View the Status & Settings window

The Status & Settings window provides a snapshot of your current protection. You can quickly see which protection features are active, identify any holes in your protection, and customize Norton Personal Firewall.

To view the Status & Settings window

1. Open Norton Personal Firewall.
2. In the Security Center, click **Status & Settings**.
3. To change any settings, double-click a protection feature.

View the Statistics window

The Statistics window provides a snapshot of your computer's *network* activity since the last time you started Windows. Use this information to identify ongoing attack attempts and review how your Privacy Control and Parental Control settings affect your protection.

The Statistics window includes information on:

Personal Firewall	Any recent attacks on this computer, including the time of the most recent attack and the address of the attacking computer
Online Content Blocking	The number of cookies, Web ads, and spam email messages that have been blocked and the number of times private information has been blocked
Parental Control	Web sites and programs that have been blocked

To view the Statistics window

1. Open Norton Personal Firewall.
2. In the Security Center main window, click **Statistics**.

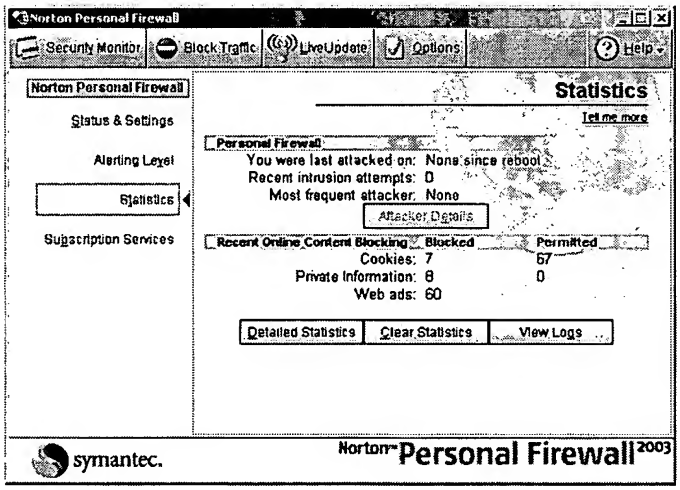
Reset information in the Statistics window

Norton Personal Firewall automatically clears all of the statistics in the Statistics window when you restart Windows. You can also clear the statistics manually. This helps you see if a configuration change affects the statistics.

To reset information in the Statistics window

1 Open Norton Personal Firewall.

2 In the Security Center, click **Statistics**.



3 In the Statistics window, click **Clear Statistics**.

Review detailed statistics

Along with the overall statistics in the Statistics window, Norton Personal Firewall maintains realtime network counters that track users' Internet usage and any actions that Norton Personal Firewall takes.

The detailed statistics include the following information.

Network	TCP and UDP bytes sent and received, the number of open network connections, and the highest number of simultaneous open network connections since the program started
Web	Graphics, cookies, and requests for browser information that have been blocked; the number of bytes and packets that have been processed; and the number of HTTP connections

Web Graphics/ Banner Ads Blocked	Estimated sizes of graphics that have been blocked, and the time saved by not loading blocked graphics
Firewall TCP Connections	The number of blocked and permitted TCP connections
Firewall UDP Datagrams	The number of blocked and permitted UDP connections
Firewall Rules	All of the rules defined for your firewall and information on the number of communication attempts blocked, permitted, or not matched by firewall rules
Network Connections	Information about current connections, including the program that is using the connection, the protocol being used, and the addresses or names of the connected computers
Last 60 Seconds	The number of network and HTTP connections and the speed of each connection type

To review detailed statistics

1. Open Norton Personal Firewall.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.

Reset detailed statistics counters

Reset the counters to clear all of the statistics and begin accumulating them again. This helps you see if a configuration change affects the statistics.

To reset counters

1. Open Norton Personal Firewall.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.
4. On the View menu, click **Reset Values**.

Set the statistics displayed in the Detailed Statistics window

Users can view all detailed statistics at once or display only certain categories.

To set the statistics displayed in the Detailed Statistics window

1. Open Norton Personal Firewall.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.
4. In the Detailed Statistics window, on the View menu, click **Options**.
5. In the Norton Personal Firewall Statistics Options window, select one or more categories of statistics that you want to display.
6. Click **OK**.

View Norton Personal Firewall Logs

Norton Personal Firewall records information about Web sites that users have visited, actions that the firewall has taken, and any alerts that have been triggered. The *logs* include details about some of the activity reported in the Statistics window.

The logs are organized onto 10 tabs.

Content Blocking	Details about banner ads, images, Java applets, and ActiveX controls blocked by Norton Personal Firewall
Connections	A history of all TCP/IP network connections made with this computer, including the date and time of the connection, the address of the computer to which you connected, the service or port number used, the amount of information transferred, and the total time the connection was active
Firewall	Communication intercepted by the firewall, including rules that were processed, alerts displayed, unused ports blocked, and AutoBlock events
Intrusion Detection	Whether Intrusion Detection is active, attack signatures being monitored, and the number of intrusions blocked
Privacy	The cookies that have been blocked, including the name of the cookie and the Web site that requested the cookie
Private Information	A history of all protected private information sent over the Internet
System	Severe system errors, the current status of IP filtering, if the logged program started as a Windows service, and information about programs that are using too many resources or otherwise operating under less than optimum conditions

Web History	URLs visited by the computer, providing a history of Web activity
Alerts	Any security alerts triggered by possible attacks on your computer
Spam	Details about emails identified as spam by Spam Alert

View the logs

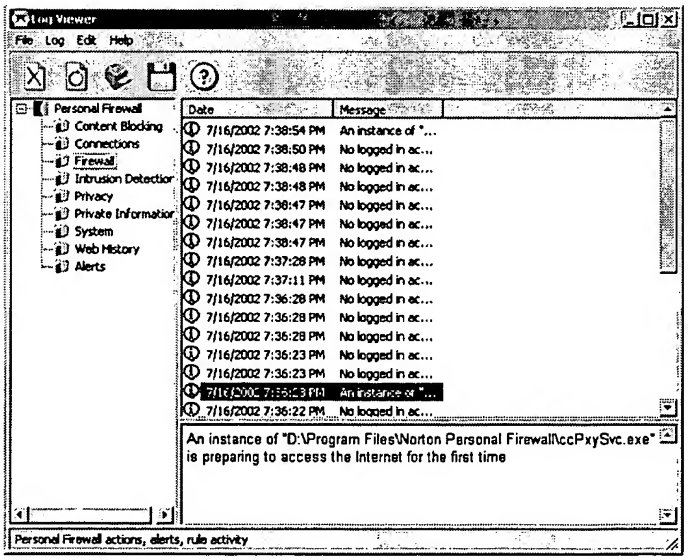
View the Norton Personal Firewall logs from the Statistics window.

To view the logs

1 Open Norton Personal Firewall.

2 Do one of the following:

- In the Security Center, click **Statistics > View Logs**.
- In the Security Monitor, on the Select a Task menu, click **View Log Viewer**.



3 In the Log Viewer, select the log that you want to review.

4 When you are done, click another log or click **OK** to close the Log Viewer.

Refresh the logs

The logs automatically refresh when you move from log to log. To view *network* events occurring since you began viewing the Log Viewer, you can manually refresh all the logs or an individual log.

To refresh all logs at once

- In the Log Viewer, right-click **Norton Personal Firewall**, then click **Refresh all Categories**.

To refresh an individual log

- In the Log Viewer, right-click the log that you want to refresh, then click **Refresh Category**.

Clear the logs

If you actively use the Internet, or if other computers frequently connect to your computer, your log files may include information about hundreds of *connections*. This can make it difficult to identify specific activity or assess the impact of any changes that you make to Norton Personal Firewall settings.

Clear the logs to remove information about past connections. This lets you see how settings changes affect your protection. You can clear a single log or clear all logs at once.

To clear a single log

1. Open Norton Personal Firewall.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, right-click the log that you want to clear, then click **Clear Category**.

To clear all logs at once

1. Open Norton Personal Firewall.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, right-click **Norton Personal Firewall**, then click **Clear all Categories**.

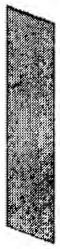
Change the size of the logs

Norton Personal Firewall stores the information for each log in a separate file. You can change the size of log files to manage the amount of hard disk space that they occupy. When the files reach their maximum sizes, new events overwrite the oldest events.

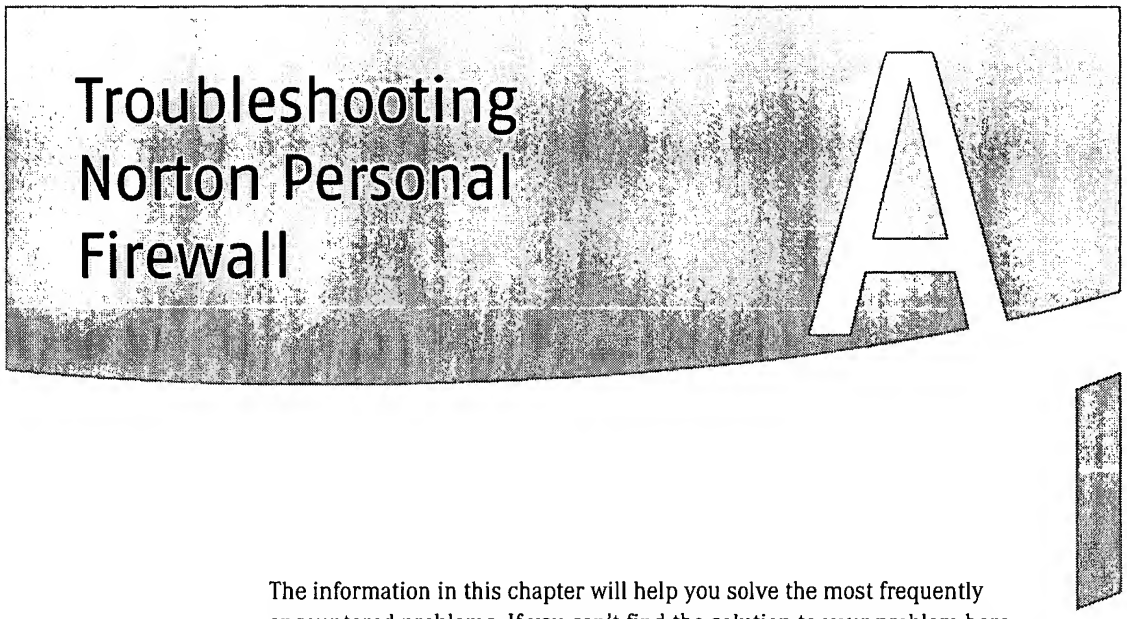
By default, log files are between 64 KB and 512 KB. If you want to see information spanning a longer period, increase the size of the log. If you need to recover hard disk space, reduce the size. Changing the size of a log file clears all of the information in that log.

To change the size of a log

1. Open Norton Personal Firewall.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, right-click a log, then click **Change Log File Size**. The Log File Size dialog box displays the Log's current file size.
5. In the Log File Size dialog box, select a new file size.
6. Click **OK**.



Troubleshooting Norton Personal Firewall



The information in this chapter will help you solve the most frequently encountered problems. If you can't find the solution to your problem here, there is a wealth of information on the Symantec Web site. You can find updates, patches, online tutorials, Knowledge Base articles, and virus removal tools.

To explore the Symantec service and support Web site

1. Point your browser to www.symantec.com/techsupp
2. On the service and support Web page, click **I am a home/small business user**.
3. On the introduction Web page, click the link for the information that you want.

If you cannot find what you are looking for using the links on the introduction page, try searching the Web site.

To search the Symantec service and support Web site

1. On the left side of any Web page in the Symantec Web site, click **search**.
2. Type a word or phrase that best represents the information for which you are looking. Use the following guidelines when searching the Symantec Web site:
   - Type a single word in lowercase letters to find all occurrences of the word, including partial matches. For example, type install to find articles that include the word install, installation, installing, etc.
   - Type multiple words to find all occurrences of any of the words. For example, type virus definitions to find articles that include virus or definitions or both.
   - Type a phrase enclosed in quotation marks to find articles that include this exact phrase.
   - Use a plus (+) sign in front of all of the search terms to retrieve documents containing all of the words. For example, +Internet +Security finds articles containing both words.
   - For an exact match, type the search words in uppercase letters.
   - To search for multiple phrases, enclose each phrase in quotation marks and use commas to separate the phrases. For example, "purchase product", "MAC", "Norton SystemWorks" searches for all three phrases, and finds all articles that include any of these phrases.
3. Select the area of the Web site that you want to search.
4. Click **Search**.

Troubleshoot Norton Personal Firewall problems

Here are some solutions to issues that might arise with Norton Personal Firewall.

What is wrong with this Web site?

Norton Personal Firewall can block certain elements of a Web site that prevent it from displaying correctly in your Web browser. In some cases, the site might not display at all.

See "Temporarily disable Norton Personal Firewall" on page 47.

If you need to view the site, disable Norton Personal Firewall and try the Web site again. Keep in mind that when you disable Norton Personal Firewall, your computer may be vulnerable to Internet attacks.

If you cannot connect to a Web site with Norton Personal Firewall disabled, there might be a problem with the Internet or your *Internet service provider*.

Problem	Solution
It could be Cookie Blocking	Many Web sites require that cookies be enabled on your computer to display correctly. See "Change the Cookie Blocking setting" on page 93.
It could be a firewall rule	A firewall rule might be blocking the Web site. When this happens, you will usually see a message saying that you could not connect. See "Customize firewall protection" on page 72.
It could be Ad Blocking	Sometimes blocking advertisements on the Internet prevents an entire Web site from appearing in your browser. See "Blocking Internet advertisements" on page 95.
It could be ActiveX or Java blocking	Some Web sites display only ActiveX controls or Java applets. If you are blocking them, nothing appears on these sites. See "Change individual security settings" on page 73.
It could be Flash blocking	Some Web sites use Macromedia Flash to create interactive front pages. If you are blocking Flash, nothing appears on these sites. See "Enable or disable Flash blocking" on page 98.

Why can't I post information online?

See "Identify private information to protect" on page 89.

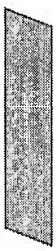
If you are unable to post information to a Web site, it may be because Privacy Control is blocking the information. Check the Private Information list in the Privacy window to see if the information that you are trying to enter is being blocked.

Why did an email message I sent never arrive?

If you choose to block an *email* message containing private information, Norton Personal Firewall immediately deletes the email message. Your email program will indicate that the message was sent, but the recipient will not receive it.

If your email program maintains copies of sent messages in its Sent or Out folder, you can reopen the email message, remove the private information, and send the message again.

Why doesn't Norton Personal Firewall notify me before letting programs access the Internet?



See "Enable Automatic Program Control" on page 76.

If Automatic Program Control is on, Norton Personal Firewall creates rules for programs that it recognizes without notifying you.

Why can't I print to a shared computer or connect to a computer on my local network?

Norton Personal Firewall blocks the use of Microsoft networking to prevent someone from connecting to your computer over the Internet.

See "Organize computers into network zones" on page 62.

To allow the use of your local network, including file and printer sharing, place the computers on your local network in the Trusted Zone.

Why can't I connect to the Internet via my cable modem?

If your network accesses the Internet via a cable *connection*, you may need to make your computer's NetBIOS name visible. While the NetBIOS name is visible, the files and folders on your computer remain hidden.

To make your NetBIOS name visible

1. Open Norton Personal Firewall.
2. In the Security Center, double-click **Personal Firewall**.
3. In the Personal Firewall window, on the Advanced tab, click **General Rules**.
4. In the General rules dialog box, click **Default Inbound NetBIOS Name**.
5. Click **Modify**.
6. In the Modify Rule dialog box, on the Action tab, click **Permit Internet access**.
7. Click **OK**.
8. In the General Rules dialog box, click **OK**.
9. In the Personal Firewall window, click **OK**.

Some Internet service providers scan the ports on users' computers to ensure that they are keeping to their service agreements. Norton Personal Firewall might interpret this as a malicious *port scan* and stop communications with your cable system. If this occurs, you need to let your cable provider run port scans.

To allow ISP port scans

1. Open Norton Personal Firewall.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the Intrusion Detection window, click **IP Address**.
4. In the Exclusions dialog box, select the IP address your ISP uses for port scans.
   Your ISP can provide this information.
5. Click **Exclude**.
6. Click **OK**.

How can a Web site get my browser information?

The Browser Privacy settings prevent your browser from sending browser information. However, some diagnostic sites on the Internet might report browser information even though the Browser Privacy settings are blocking it.

If you are blocking *Java*, *ActiveX*, or scripts, the site might be using one of these methods to retrieve the information. Sometimes when Web servers do not get the information from the browser, they use the last piece of browser information that they received instead. You might see the information from the last person who viewed the site.

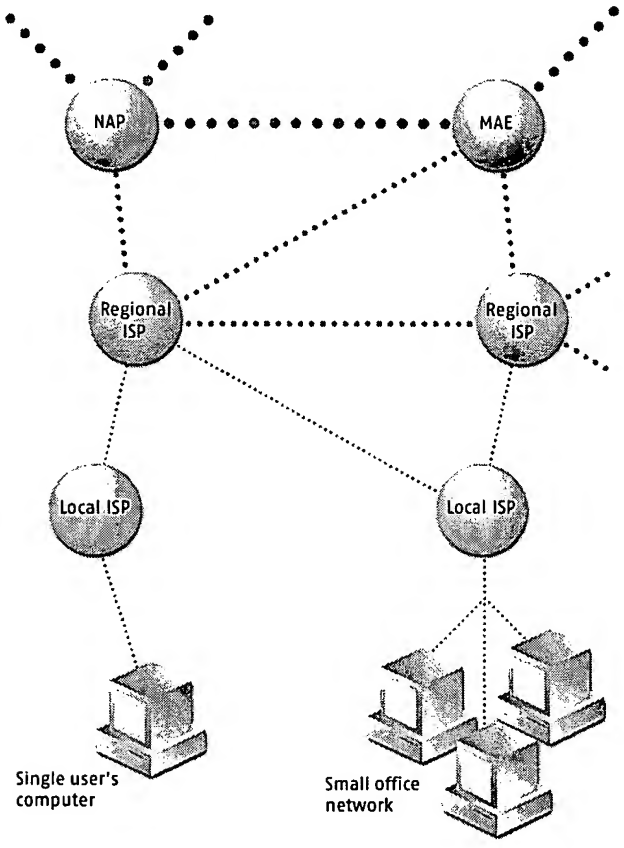
About the Internet

B

The Internet is the interconnection of millions of computers throughout the world. It is comprised of the computers and the connections that make it possible for any computer on the Internet to communicate with any other computer on the Internet.

The Internet is analogous to a system of roads and highways. The superhighways of the Internet, called the Internet backbone, carry large amounts of information over long distances. There are interchanges on the backbone, called network access points (NAPs) and metropolitan area

exchanges (MAEs). There are regional highways provided by large ISPs and local streets provided by local ISPs.



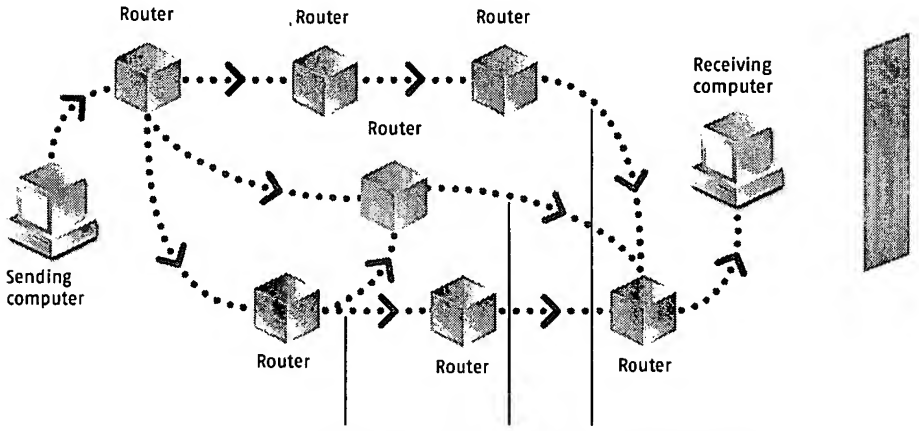
Like a system of roads and highways, the Internet provides multiple routes from one point to another. If one part of the Internet has too much traffic, or is damaged, information is rerouted.

How information is transmitted over the Internet

All information sent over the Internet is communicated using a protocol called *TCP/IP*. Because all of the computers on the Internet understand this protocol, each one can communicate with every other computer on the Internet. TCP and IP are separate parts of this protocol.

The Internet is a *packet switching network*. Every communication is broken into *packets* by TCP (Transmission Control Protocol). Each packet contains the addresses of the sending and receiving computers along with the information to be communicated.

IP (Internet Protocol) is responsible for routing the packets to their destinations. Each packet may take a different route across the Internet, and packets may be broken up into *fragments*. Packets travel across the Internet, moving from one *router* to another. Routers look at the destination address and forward the packet to the next router. IP does not guarantee the delivery of every packet.



Routes that a packet or fragments of a packet may take

On the destination computer, TCP joins the packets into the complete communication. TCP may have to reorder the packets if they are received out of order, and it may have to reassemble fragmented packets. TCP requests retransmission of missing packets.

TCP/IP is often used to refer to a group of protocols used on the Internet, including UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), and IGMP (Internet Group Membership Protocol).

About UDP

UDP (User Datagram Protocol) is used for functions in which the reliability of TCP is not necessary, such as broadcasting video to multiple computers at once. UDP doesn't provide error correction or retransmission of lost packets. UDP is secondary in importance to TCP when you browse the Internet.

About ICMP

ICMP (Internet Control Message Protocol) packets contain error and control information. They are used to announce network errors, network congestion, timeouts, and to assist in troubleshooting.

Norton Personal Firewall normally allows inbound ICMP packets that provide you with information and are a minimal security risk. You can create rules to block some or all ICMP packets.

About IGMP

IGMP (Internet Group Membership Protocol) is used to establish memberships in multicast groups, collections of computers that receive simultaneous messages from a single computer. Typically, IGMP is used to broadcast video and other multimedia over the Internet. Your computer reports to a nearby router that it wants to receive messages addressed to a specific multicast group.

IGMP does not present a major security risk, but Norton Personal Firewall allows you to block the protocol entirely. This is a good idea if you do not use any programs that require IGMP. If you have problems receiving multicast information, such as movies or PowerPoint presentations, be sure that IGMP is not blocked.

How Web information is located on the Internet

Web information is stored as pages, each with a unique name called a *URL (Uniform Resource Locator)*.

When you type a Web address in the browser address bar or click a link in your Web browser to move to a new Web site, you are giving your browser the URL of the page that you want to view. For example, www.symantec.com is a typical URL.

Each URL maps to the IP address of the computer that stores the Web page. URLs are used because they are easier to remember and type than IP addresses.

Before your browser requests a page, it asks a *DNS (Domain Name System) server* for the IP address of the Web site. IP addresses are 32-bit numbers expressed as four decimal numbers, each ranging from 0 to 255, and separated by periods: 206.204.104.148. Every computer on the Internet has a unique IP address.

Requesting a page

Once the browser has the IP address, it establishes a TCP *connection* to the Web server and requests the page. Each page that you view requires a new connection with the Web server. In fact, most pages require multiple connections, since each graphic (as well as many other page elements) requires its own connection.

Once a page is loaded, all of the connections are dropped. The process starts over for each page on the site, though your browser does remember the site's IP address. Some newer Web sites use HTTP 1.1 (Hypertext Transfer Protocol version 1.1) to establish a single connection that can pass multiple files and stay open for multiple pages.

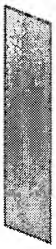
Understanding URLs

A typical URL looks like this: http://www.symantec.com/securitycheck/index.html. Because you might want to block some parts of a *domain* while allowing other parts of the same domain, you should understand the parts that comprise a URL.

http://	The program protocol used to make the connection. The most common protocol for browsing the Web is HTTP (Hypertext Transfer Protocol). Your browser assumes that this is the program protocol if you don't enter one. Other commonly used protocols include FTP (File Transfer Protocol) and gopher.
.com	The root or top-level domain. There are several familiar root domains, including .com, .net, .edu, .org, .mil, and .gov. There are also two-letter root domains for most countries, such as .ca for Canada and .uk for the United Kingdom.

symantec.com	The domain. This is the domain with which the browser establishes a connection. A domain frequently refers to a single company or organization that might have multiple Web sites on the Internet.
www.symantec.com	The host. This is the particular Web site with which the browser communicates. It is also the name for which DNS provides an IP address.
securitycheck	The folder or directory that contains the file to be accessed.
index.html	The file name of the file to be accessed.

There is one particular URL that identifies your computer to itself, and that is localhost. If your computer has Web server software installed, you can type http://localhost and see your Web page. The IP address that corresponds to localhost is 127.0.0.1.



How ports identify programs on servers

Ports, also called *sockets*, provide the locations of particular programs or servers on the remote computer with which you are trying to establish communication. This makes it possible to run multiple Internet programs simultaneously on a single computer. For example, many computers on the Internet run both Web and FTP servers. The Web server uses port 80, while the FTP server uses port 21.

Ports are numbered 1 through 65535. Ports 1 through 1023 are known as well-known ports and are the default ports for many common Internet programs.

Ports are part of *URLs*, but they are rarely seen. The *port number* follows the host name and a colon. For example:

http://www.symantec.com:80/securitycheck/index.html

Because the most-used ports are standardized, you rarely see port numbers. For example, Web browsers almost always use port 80, so they don't require that you type it unless you need to use a different port.

The terms server and *service* are used somewhat interchangeably. For example, a Web server provides the HTTP service, while it is usually said that a computer has the *finger* service running.

Well-known ports

Following are some of the most common well-known ports.

Default port	Service name	Program
20	ftp-data	FTP (File Transfer Protocol) data
21	ftp	FTP (File Transfer Protocol) control
23	telnet	Telnet terminal handler
25	smtp	SMTP (Simple Mail Transfer Protocol)
53	domain	DNS (Domain Name Service) lookup
79	finger	Finger
80	http	HTTP (Hypertext Transfer Protocol)
110	pop3	POP3 (Post Office Protocol 3)
113	auth	Ident Authentication Service
119	nntp	NNTP (Network News Transfer Protocol)
137	nbname	NetBIOS name (Microsoft Networking)
138	nbdatagram	NetBIOS datagram (Microsoft Networking)
139	nbsession	NetBIOS session (Microsoft Networking)
143	imap	IMAP (Internet Message Access Protocol)
194	irc	IRC (Internet Relay Chat)
389	ldap	LDAP (Lightweight Directory Access Protocol)
443	https	HTTPS (Secure HTTP)

How computers are identified on the Internet

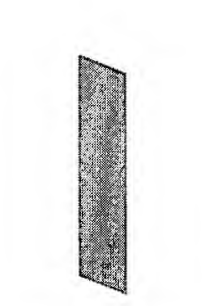
Millions of computers are connected to the Internet. When you are trying to identify computers, it is easier to work with groups of computers rather than having to identify each one individually. *Subnet* masks provide a way to identify a group of related computers, such as those on your local network.

A typical subnet mask looks like this: 255.255.255.0. The 255s indicate parts of the IP address that are the same for all computers within the subnet, while the 0 indicates a part of the IP address that is different.

Subnet masks are always used in conjunction with base IP addresses. The base IP address is an IP address that, when processed using the subnet mask, can indicate all of the IP addresses in a subnet.

A typical base IP address/subnet pair looks like this:

Base IP address:	10.0.0.1
Subnet mask:	255.255.255.0



In this example, the range of IP addresses that the base IP address and subnet mask identify range from 10.0.0.1 to 10.0.0.255. The most common subnet mask used is 255.255.255.0 because it identifies a relatively small group of IP addresses, up to 254 computers. It is commonly used for very small groups of computers, including groups as small as two computers.

Understanding Internet risks

Norton Personal Firewall protects you from major risks that are associated with the Internet. These risks include the threat of network attack, malicious code in *active content*, exposure to inappropriate content, exposure of private information, and getting viruses from infected files.

Risks from hackers

Originally *hackers* were people who could solve computer problems and write complex computer programs quickly. However, the meaning of the term has changed to mean those who use their computer knowledge for illicit purposes. Since hacker started out as a complimentary term, some people use the word *cracker* for the derogatory form. In this text, hacker is used in its noncomplimentary form.

You might also hear other terms for hackers, including script-kiddies, wannabes, and packet monkeys. These are all terms for hackers-in-training, who use programs written by more advanced hackers to attack computers on the Internet.

The process of a hacker attack

Most hacker attacks use the following process:

- Information gathering
  The hacker gathers as much information about your computer as possible. The hacker attempts to find vulnerabilities without letting you know that your computer is under attack.

- Initial access
  The hacker exploits a vulnerability found during information gathering and establishes an entry point into your computer.
- Privilege escalation
  The hacker gains access to more programs and *services* on your computer.
- Covering tracks
  The hacker hides or removes evidence of the intrusion, sometimes leaving an entry point open for return.

Information gathering

The first step in information gathering is acquiring a target. A hacker can choose a person or company to attack, or search the Internet for an unprotected target that will be easy to hack. The amount of information available about you on the Internet is directly related to your level of Web presence. If you have a *domain* name and a Web site, more information is publicly available than would be if you only had an *email* address.

If a hacker has chosen a specific target, such as a company or organization, many resources on the Internet assist in gathering information. Using the Internet, a hacker can learn a lot about a potential target. Given a domain name, it's easy to find out the name and address of the owner, as well as the name and phone number of the administrative and technical contacts. While this information usually can't be used directly to attack a network or computer, it can be used to gather more information.

If a hacker doesn't have a specific target in mind, many tools are available for scanning the Internet and finding possible targets. The simplest scan is a ping scan, which can quickly scan thousands of computers. The hacker uses a program to ping computers at a series of IP addresses. A response tells the hacker that a computer exists at an IP address. When Norton Personal Firewall is running, your computer is hidden from ping scans because your computer does not respond. The hacker does not learn that there is a computer at your IP address by pinging it.

Port scans are more comprehensive and are usually performed on single computers. A port scan can tell a hacker which services are running, such as HTTP and FTP. Each service that is running provides a potential entry point for the hacker. On unprotected computers, unused ports respond that they are closed, telling the hacker that a computer exists at that IP address. Norton Personal Firewall does not respond to scans of unused ports, giving them a *stealth* appearance.

Initial access

The easiest way for a hacker to access a Windows computer is to use Microsoft networking. On many computers, Microsoft networking is enabled so that anyone on the network can connect to it.

Microsoft NetBIOS networking uses three of the well-known ports. These ports are used to establish *connections* among computers on a Microsoft network. In fact, they normally advertise the name of your computer over the local network. This is what you want on your own network, but it is not what you want on the Internet. Norton Personal Firewall is preset to block these ports and prevent someone on the Internet from connecting to your computer using Microsoft networking. If your computer is connected to a local network as well as to the Internet, you must change some settings to allow communication with the other computers on your network. Norton Personal Firewall still protects you from Internet risks while allowing you to use your local network.

Privilege escalation

Once a hacker has connected to your computer, the next step is to gain as much control as possible. The steps involved and the results obtained vary depending on the version of Windows that is running on the target computer.

On computers running Windows 95/98/Me, once hackers have gained access to the computers, there is no need for escalation. They have full control of the computers. Luckily, these versions of Windows don't have many remote control features, so they are relatively easy to protect.

On computers running Windows 2000/XP, hackers attempt to gain administrative rights to the computers. The key to getting administrative rights is usually a *password*. The hacker can download your password file and decode it.

Another tactic is to place a *Trojan horse* on your computer. If a hacker can place a program such as Back Orifice, Subseven, or NetBus on your computer and run it, it is possible to take control of the computer.

Other Trojan horses might record all of your keystrokes to capture passwords and other sensitive data. Norton Personal Firewall and Norton AntiVirus provide two levels of protection against Trojan horses. Norton AntiVirus protects you from inadvertently running these programs. Norton Personal Firewall blocks the ports that remote access Trojan horses use to communicate over the Internet.

Other Trojan horse programs might record all your keystrokes to capture passwords and other sensitive data. Norton Personal Firewall blocks the ports that Remote Access Trojan horse programs use to communicate over the Internet.

Covering tracks

When a hacker has gained as much control of a computer as possible, the task turns to concealing the evidence. If you don't know that a hacker has compromised your computer, you won't take steps to stop such actions.

On computers running Windows 2000/XP, hackers try to turn off auditing and modify or clear the event *logs*. On any computer, hackers may hide files so that they are available for future visits. In extreme cases, hackers might format the hard drive of a compromised computer to avoid identification.

Risks from active content

ActiveX controls and *Java applets* are called *active content* because they can do more than display text or graphics. Most active content is safe. Common uses of active content are popup menus and up-to-date stock quotes.

Both ActiveX and Java are supposed to be safe to run in your browser. ActiveX uses a system of digital certificates that lets you decide if you want an ActiveX control to run. Digital certificates appear as dialog boxes that ask if you want to install and run a control that appears when you are browsing the Web.

There are several problems with using digital certificates. Some controls do not have certificates, and some certificates provide very little information about what the control does.

The Java sandbox was designed to prevent Java applets from accessing information outside of the browser and doing anything that might harm your computer. However, *hackers* continually find ways to get around Java safeguards and use Java features in ways not conceived of by its developers.

Norton Personal Firewall monitors active content and can block all active content or warn you whenever active content is encountered. Norton AntiVirus Auto-Protect detects malicious ActiveX controls and Java applets and prevents them from running.

Norton Personal Firewall monitors active content and can block all active content or warn you whenever active content is encountered.

Risks from inappropriate content and activities

There is a wealth of information on the Internet that is easily accessible to everyone. However, some topics are not suitable for all people. For example, most people consider pornographic and violent sites to be inappropriate for viewing by children. You may feel that other topics should also be off limits.

Blocking site and newsgroup categories

Norton Personal Firewall lets you choose Web sites and newsgroups that you want to be accessible to people using this computer. Because different people need different levels of access, you can configure Norton Personal Firewall to block specific content for each user.

Restricting access to programs

Some Internet-enabled programs might be inappropriate for use on your computer. For example, you may not want children using realtime chat programs. You may also want to restrict the use of file transfer programs. This reduces the risk of introducing viruses, worms, zombies, *Trojan horses*, or other malicious code onto your computer or network.

Norton Personal Firewall lets you choose categories of programs that can access the Internet. It keeps the list of programs up-to-date, so your protection stays current as new programs are released. You can also add custom programs, and control their uses as well.

Risks to your privacy

The Internet presents several risks to your privacy. Some sites collect and save personal information, such as credit card numbers. Some sites track your Internet usage. Some programs send information about your computer usage to Web sites without your permission.

Sending private information

You probably don't want private information, such as credit card numbers or your home phone number, to be sent unencrypted over the Internet. Privacy Control prevents private information from being entered on Web sites that do not use secure, encrypted communications, and from being sent on instant messenger programs.

You may want to prevent some users from sending private information over the Internet. Norton Personal Firewall can block users from accessing secure sites where they might be asked for personal information.

Understanding cookies

Cookies are messages sent to your browser by Web sites that are stored as small files on your computer. They are often used by Web sites to track your visits. In most cases, cookies do not contain personal information, but instead carry information that identifies you to Web sites.

Good cookies

In their most benign form, cookies last only until you close your browser. This type of cookie is mainly used to remember choices that you make as you navigate through a Web site.

Many sites leave cookies on your computer so that they recognize you when you return to their sites. These cookies identify you so that options that you have chosen in the past are used for your current visit to the site. If you frequent a site that remembers the stocks that you want to track, for example, it probably uses this kind of cookie.

Bad cookies

In one of their malevolent forms, cookies from one Web site might track your visits to a different Web site. For example, most of the ads that you see on Web sites do not come from the site that you are viewing, but from sites that provide ads to many sites. When the advertising site displays the ad, it can access cookies on your computer. This lets the advertising company track your Web usage over a range of sites and profile your browsing habits.

Blocking cookies

Norton Personal Firewall can block all cookies or it can notify you of each cookie request. If you block all cookies, you lose functionality at many Web sites. For example, you might be blocked from making purchases at some Internet stores. If you choose to be prompted each time that a Web site tries to create a cookie, you can evaluate each request and block those that are not from the site that you are viewing. Norton Personal Firewall can block or allow cookies from particular *domains* or Web sites.

Tracking Internet use

Most browsers pass on information that you might want to keep confidential. One item that your browser normally passes to Web sites is the *URL* of the page from which you came. This information is used by some Web sites to help you navigate through the Web site, but it can also be used to track your Web usage. Norton Personal Firewall blocks this information.

Your browser also sends information about itself and the operating system that you are using. While Norton Personal Firewall can block this information, it is usually used by Web sites to provide Web pages that are appropriate for your browser.

A more sinister invasion of your privacy is found in programs that you install on your computer that, without your knowledge, report information back to Web sites. Several programs that help you download and install files report your activities over the Internet. Norton Personal Firewall protects your privacy by alerting you to these communications.

Risks from Trojan horses and viruses

With so many computers connected by networks and the Internet, viruses can spread more rapidly than they could in the days when files were transferred from computer to computer on disks. Additionally, the risk has broadened from viruses to *Trojan horses*, worms, and zombies.

A virus is a program or code that replicates by attaching itself to another program, a boot sector, a partition sector, or a document that supports macros. Many viruses just replicate, but others do damage. A virus can arrive in a document that you receive by *email*.

A Trojan horse is a program that does not replicate, but damages or compromises the security of the computer. Typically, it relies on someone emailing it to you; it does not email itself. A Trojan horse may arrive disguised as useful software. Some Trojan horses perform malicious actions on the computer on which they are run, while others, such as Back Orifice, provide remote control capabilities for *hackers*.

A worm is a program that makes copies of itself, for example, from one disk drive to another, or by sending itself through email. It may do damage or compromise the security of the computer. A worm can arrive as an attachment to an email that has a subject that tempts you to open it.

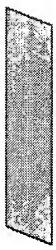
A zombie program is a dormant program secretly installed on a computer. It can later be run remotely to aid in a collective attack on another computer. Zombie programs don't normally damage the computer on which they reside, but are used to attack other computers. A zombie program can arrive as an email attachment.

Norton AntiVirus protects you from receiving and executing viruses, Trojan horses, worms, and zombies. Norton AntiVirus scans email as you receive it and also checks files when you open them, providing two levels of protection.

Norton Personal Firewall ensures that Trojan horses do not communicate over the Internet. This means that you are protected from hackers who use Trojan horses.

The likelihood of being attacked

The Internet presents many risks. What are the odds that your computer will be attacked? The chance of an attacker singling out your computer from all of those on the Internet is slim. However, the use of port-scanning and other computer discovery tools by hackers means that your computer may be scanned relatively frequently for vulnerabilities. The more vulnerabilities that are found, the more inviting your computer is to hackers.



The tools that hackers use to find targets can scan large groups of computers on the Internet. The hacker simply enters a range of IP addresses to be scanned. The program checks each IP address in the range to see if a computer is there. If it finds a computer, it performs a series of tests to identify vulnerabilities, such as having Microsoft networking enabled over the Internet. The hacker returns to find a list of computers and their vulnerabilities.

Norton Personal Firewall protects you from these scans by making your computer invisible. Your computer won't respond to queries that these scanners send. This means that your computer exhibits no vulnerabilities to the hacker, making it a poor target for attack.

Glossary

This glossary provides definitions of some common Internet terms.

active content	Material on a Web page that changes with time or in response to user action. Active content is implemented through ActiveX controls, Visual Basic Scripts, Java scripts, and Java applets in the HTML code that defines the page.
ActiveX control	A program that runs within a browser using Microsoft technology to add life to a Web page by using animation, streaming audio and video, movies, and so on. When you visit a Web page that contains an ActiveX control, it is dynamically downloaded and saved to your hard disk. Unlike Java applets, ActiveX controls don't run in a restricted environment, and have the potential to take control of your computer.
alert	A dialog box that appears in a graphical user interface (GUI) to signal that an error has occurred, or to provide a warning.
banner ad	An advertising graphic, often animated, that appears on a Web page and may contain a link to the advertiser's Web site.
browser	A software application that makes navigating the Internet easy by providing a graphical user interface. This lets the user click menus, icons, or buttons rather than learn difficult computer commands. Also called a Web client.

connection	A method of data exchange that allows a reliable transfer of data between two computers.
connection attempt	The data transfer that requests the opening of a connection.
cookie	A small data file that some Web sites place on your hard disk while you're viewing a Web page. Web servers can use cookies to store your personal information and preferences so that you don't need to reenter them each time that you visit.
cracker	A person who cracks code, not necessarily for malicious reasons. Sometimes used to refer to a malicious hacker.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that automatically assigns a temporary IP address to each device on a network.
DNS (Domain Name System)	A hierarchical naming system that translates domain names (such as www.symantec.com) into IP addresses (such as 206.204.212.71).
DNS server (Domain Name System server)	A computer that keeps a database of domain names and their corresponding IP addresses. When a computer sends a domain name to a DNS server, the server returns the IP address for that domain.
domain	The common address for a single company or organization (such as symantec.com) on the Internet, which might have multiple hosts.
download	To transfer data from one computer to another, usually over a modem or network. Usually refers to the act of transferring a file from the Internet, a bulletin board system, or an online service to one's own computer.

email (electronic mail)	A method of exchanging messages and files with other people via computer networks. A popular protocol for sending email is SMTP (Simple Mail Transfer Protocol). Popular protocols for receiving email are POP3 (Post Office Protocol 3) and IMAP4 (Internet Message Access Protocol 4). Web-based email services use HTTP (Hypertext Transfer Protocol) for sending and receiving email.
finger	A command in some operating systems that requests network user account information.
firewall	A security system that uses rules to block or allow connections and data transmissions between your computer and the Internet.
firewall rule	A set of parameters that specifies a type of data packet or network communication and an action to perform (permit it or block it) when it is found.
fragment	An IP packet that has been split into two or more parts, or fragments. When the size of an IP packet exceeds the maximum frame size of a network that it crosses, the packet must be divided into smaller packets, or fragments.
hacker	A person who attempts unauthorized access of other people's computers for the purpose of obtaining information from, or doing damage to, those computers.
HTML (Hypertext Markup Language)	A standard language for documents on the World Wide Web. Codes inserted in a text file instruct the Web browser on how to display a Web page's words and images for the user, and define hypertext links between documents.
inbound communication	An attempt by an external computer to open a connection to your computer. The connection can be used to send data to and from your computer.
IP (Internet Protocol)	The essential protocol by which data is sent from one computer to another on the Internet. IP routes packets to the appropriate destinations.

IP address (Internet Protocol address)	A 32-bit numeric identifier that uniquely identifies a computer on the Internet. IP addresses are usually expressed as four groups of numbers, each ranging from 0 to 255, separated by periods. For example, 206.204.52.71.
ISP (Internet service provider)	A company that supplies Internet access to individuals and companies. Most ISPs offer additional Internet connectivity services, such as Web site hosting.
Java applet	A small program that runs in a restricted environment, sometimes referred to as a sandbox, that is managed by your browser. Most Java applets are used to add multimedia effects, interactivity, or other functionality to a Web page, but they can also be used for malicious purposes, such as password theft.
JavaScript	A scripting language that is similar to, but less capable than, Java. JavaScript code can be included in Web pages to add interactivity and other functionality.
local	A term that refers to your computer, as opposed to a remote computer.
log	A record of actions and events that take place on a computer or handheld device.
modem	A device that modulates (converts to analog) and demodulates (converts from analog) digital data for transmission over a telephone line. Also includes interface devices for digital connections to the Internet, such as ISDN, cable, and DSL.
network	A set of computers and associated hardware connected together in a work group for the purpose of sharing information and hardware among users.
NAT (network address translation)	A method of converting IP addresses used on an intranet or local area network into Internet IP addresses. This lets many computers share an Internet IP address. More importantly, it hides the IP addresses of network computers from outsiders.

network address	The portion of an IP address that is common to all computers on a particular network or subnet.
operating system	A program that ties the capabilities of computer hardware and software to input/output devices such as disks, keyboards, and mouse devices.
outbound communication	An attempt by your computer to open a connection with a remote computer. The connection can be used to send data to and from your computer.
packet	A unit of data that is routed between an origin and a destination on the Internet. In addition to the data being transmitted, a packet contains information that enables computers on a network to determine whether to receive it.
packet-switching network	A network of computers (such as the Internet) that transmits files by breaking them into packets and routing each packet along the best available route between the source and destination computers.
password	A character sequence entered by users to verify their identities to a network or program. The most secure passwords are difficult to guess or find in a dictionary, and contain a combination of capital letters, lowercase letters, numbers, and symbols.
POP3 (Post Office Protocol 3)	An email protocol used to retrieve email from a remote server over an Internet connection.
port	A transport user identification used by a client program to specify a particular server program on a computer. Also called service. Some applications have ports with preassigned numbers. Others are assigned port numbers dynamically for each connection. When a service (server program) is started, it binds to its designated port number. When a client program wants to use that server, it also must request to bind to the designated port number.

port number	A logical communications channel to be used by a particular TCP/IP application. Each application has unique port numbers associated with it. By convention, some protocols use a well-known port number (for example, HTTP uses port 80), although this is configurable.
port scan	An attempt to gain access to a computer by searching for open ports. Usually done by an automated program that sends a request to each port at an IP address, listening for responses that could reveal a vulnerability.
proxy	A mechanism that lets one system act on behalf of another system when responding to protocol requests. Security programs in firewalls use proxy services to screen the secured network from users on the Internet.
router	A device on a network that links computers or interconnected networks. A router receives packets and forwards them to their destination via the best available route.
server	The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.
service	Protocols that let one computer access a type of data stored on another computer. Many host computers that are connected to the Internet offer services. For example, HTTP servers use the Hypertext Transfer Protocol to provide World Wide Web service and FTP servers offer File Transfer Protocol services. See also port.
socket	An identifier for a particular service on a particular computer. A socket consists of the IP address of the computer followed by a colon and the port number.
stealth	Giving the impression of not existing by not responding to requests for information.
subnet	A local area network that is part of a larger intranet or the Internet.

TCP/IP (Transmission Control Protocol/ Internet Protocol)	The standard family of protocols for communicating with Internet devices.
threat	A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/ or denial of service.
timeout	A predetermined period of time during which a given task must be completed. If the timeout value is reached before or during the execution of a task, the task is canceled.
top-level domain	The last part of a domain name that identifies the type of entity that owns the address (such as .com for commercial organizations or .edu for educational institutions), or the geographical location of the address (such as .ca for Canada or .uk for United Kingdom).
Trojan horse	A destructive program that is often designed to cause damage to a computer, while disguised as something useful or interesting.
URL (Uniform Resource Locator)	The global address of documents and other resources on the World Wide Web and the convention that Web browsers use to locate files and other remote services.
Web page	A single document on the World Wide Web (WWW) that is identified by a unique URL. A Web page can contain text, hyperlinks, and graphics.
Web site	A group of Web pages that is managed by a single company, organization, or individual. A Web site may include text, graphics, audio and video files, and hyperlinks to other Web pages.
World Wide Web (WWW)	The collection of hypertext documents that are stored on Web servers around the world. Also called WWW or simply the Web. The Web allows universal access to a vast collection of documents that are stored in HTML format as Web pages.

Service and support solutions

The Service & Support Web site at http://service.symantec.com supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at http://service.symantec.com tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at:
http://www.symantecstore.com

Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- Online Service and Support
  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.
- PriorityCare telephone support
  This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at:
http://service.symantec.com

Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Latin America

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12 andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

Portuguese:
http://www.service.symantec.com/br
Spanish:
http://www.service.symantec.com/mx
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)
Argentina: +54 (11) 5382-3802

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

July 25, 2002

Index

J

L

N

O

P

R

S

T

U

V

W

Z

Norton™ Personal Firewall

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE. You must be a registered customer in order to receive CD replacements.

If your Symantec product was installed on your computer when you purchased it, contact your hardware manufacturer for CD replacement information.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name _____

Company Name _____

Street Address (No P.O. Boxes, Please) _____

City _____ State _____ Zip/Postal Code _____

Country* _____ Daytime Phone _____

Software Purchase Date _____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem: _____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	
Shipping & Handling	$ 9.95
TOTAL DUE	_____

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%).
Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _____ __ Visa __ Mastercard __ AMEX

Credit Card Number _____ Expires _____

Name on Card (please print) _____ Signature _____

**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
555 International Way
Springfield, OR 97477 (800) 441-7234
Please allow 2-3 weeks for delivery within the U.S.

symantec.

APPENDIX B

INVESTIGATION OF CLAIM 1 OF U.S. PATENT APP. SER. NO.: 10/071,549

Claims 1 and 13 of U.S. Patent App. Serial No. 10/071,549		Symantec's Personal Firewall
1.	A method for tracing a traffic event utilizing a firewall, comprising:	Symantec's Personal Firewall provides a method for tracing a traffic event utilizing a firewall. See excerpt(s) below. "You can trace *connection attempts* from three places in Norton Personal Firewall:" See page 43 of Norton Personal Firewall 2003 Manual.pdf.
(a)	executing a firewall on a local computer;	Symantec's Personal Firewall executes or induces one to execute a firewall on a local computer. See excerpt(s) below. "To access Norton Personal Firewall: Do one of the following: On the Windows taskbar,click **Start >Programs >Norton Personal Firewall >Norton Personal Firewall."** See page 35 of Norton Personal Firewall 2003 Manual.pdf.
(b)	monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;	Symantec's Personal Firewall monitors traffic events between the local computer and a remote computer over a network. See excerpt(s) below. "Norton Personal Firewall monitors communications." See page 7 of Norton Personal Firewall 2003 Manual.pdf.
(c)	displaying the traffic events utilizing the firewall;	Symantec's Personal Firewall displays the traffic events utilizing the firewall. See excerpt(s) below. "When Visual Tracking is finished,it displays a visual representation of where this communication originated and contact information for the owner of the IP address." See page 44 of Norton Personal Firewall 2003 Manual.pdf.
(d)	tracing at least one of the traffic events utilizing the firewall; and	Symantec's Personal Firewall traces at least one of the traffic events. See excerpt(s) below. "You can trace *connection attempts* from three places in Norton Personal Firewall:" See page 43 of Norton Personal Firewall 2003 Manual.pdf.
(e)	displaying a map of the trace utilizing the firewall.	Symantec's Personal Firewall displays a map of the trace. See excerpt(s) below.

		"**NEW!** Visual Tracking displays the source of an attack on a world map." See Norton Personal Firewall 2003 Advertising.pdf.
13.	A computer program product for tracing a traffic event utilizing a firewall, comprising:	Claim 13 is the software analog to Claim 1. The above product includes a computer program product for tracing a traffic event, as set forth in Claim 1. See excerpts above.
(a)	computer code for executing a firewall on a local computer;	
(b)	computer code for monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;	
(c)	computer code for displaying the traffic events utilizing the firewall;	
(d)	computer code for tracing at least one of the traffic events utilizing the firewall; and	
(e)	computer code for displaying a map of the trace utilizing the firewall.	